Accountability for the Digital Age

Modernizing Nova Scotia's Access & Privacy Laws

A Report by the
Information and Privacy Commissioner for Nova Scotia

June 2017

Executive Summary

Effective access to information rights and strong privacy protections promote the common good and support human flourishing. Nova Scotians deserve and expect to have a robust, modern law to protect these essential rights. But twenty-four years ago, when Nova Scotia last updated its access and privacy law, the world was a different place. In 1993 there were only 130 websites. Today there are one billion. Google wasn't founded until 1998 and Facebook wasn't created until 2004. Big data was the realm of scientists and dreamers.

The digital age is upon us and our laws are quite simply no longer up to the task. Significant improvements are required to bring our access and privacy rights into the 21st century. There are four core areas of weakness in Nova Scotia's access and privacy laws.

Modernizing Access Rights: One key weakness of our current access law is that it fails to enshrine a right to receive information in an electronic format so that the data is open, reusable and accessible. Further, modern democracies have embraced open government as a means of ensuring transparency in decision making. To protect and advance these efforts it is important to have statutory provisions that support open government as a citizen's right. Another key modern access provision is a legal obligation to create records in the first place. A right to access government information is meaningless if no record exists. Finally, Nova Scotia has the weakest public interest override of any Canadian jurisdiction. Such a right ensures that, no matter what exemption is claimed, public bodies must always consider whether or not disclosure would nonetheless be in the public interest.

I recommend a number of significant improvements to access provisions including:

- Give a right to access records in a format that is open, reusable, and accessible.
- Add open government obligations including publication requirements and a reporting requirement.
- Create a statutory duty to document.
- Modernize exemptions by placing time limits on each and by subjecting exemptions to a final public interest test.
- Remove the $5 application fee.
- Protect applicant identity.

Modernizing Privacy Rights: Nova Scotia's privacy laws lack virtually all of the essential modern privacy protections found in other Canadian jurisdictions. The need for these privacy protections has grown exponentially thanks to two key developments: the arrival of big data and increased expectations from citizens that government entities respond to citizens' needs first, and bureaucratic borders second. Government entities want to use big data for the benefit of citizens. They want to work together to deliver integrated programs and activities for the benefit of citizens and in response to their demands. Privacy rules affect their ability to do so. But privacy rules can facilitate their ability to do so when the laws include clear processes and strong privacy protections so the services can be created and delivered while privacy rights remain secure.

Without these essential modern privacy protections, databases of citizen information are not adequately protected for the 21st century. Fundamental privacy protections that enable innovation in government services include mandatory requirements for privacy impact assessments, information sharing agreements, mandatory breach notifications, and consultations on draft legislation. Nova Scotia's laws also need to include privacy management program requirements,

requirements for collection notification, and effective provisions to ensure that public bodies create an inventory of all of the personal information they collect about citizens.

I recommend improvements in nine areas of the law including:

- Update the standards of sharing personal information to allow for big data projects and common or integrated programs or activities – subject to mandatory privacy impact assessment requirements and appropriate notification to the Information and Privacy Commissioner.
- Add core privacy standards into our laws: require that government entities use personal information only when necessary, use the least amount of personal information possible, and limit internal sharing to a need-to-know basis.
- Make privacy impact assessments, information sharing agreements, and breach notification all mandatory in prescribed circumstances.
- Add a requirement that public bodies and municipalities have a privacy management program that includes policies, practices, and training.
- Require notification to individuals when their personal information is collected.
- Require the creation of publicly available personal information banks so citizens know what information is collected about them, how it is used, and why it is disclosed.

Improving Oversight: One of the core purposes of access and privacy law is to allow for independent oversight of government decisions. There are a variety of core elements of independence missing in Nova Scotia's model. I recommend improvements in 11 areas including:

- Make the Commissioner an officer of the legislature.
- Grant the Commissioner independence in relation to employees, experts, support, and delegation equivalent to other officers in Nova Scotia.
- Require public bodies to obtain the court's permission if they wish to decline to follow a recommendation of the Commissioner.
- Rationalize the Commissioner's powers so that she has the same authority with respect to all public bodies and municipal bodies whether the issue is access or privacy.

Organization and Coverage: There is a confusing array of laws governing this area. Having four separate access and privacy laws does not make sense to citizens. Their expectations with respect to their rights to access information or to protection of their personal information is the same no matter what level of government has the information. One streamlined, consistent law for all government bodies would be more accessible and comprehensible for citizens and the public bodies themselves.

Added to this issue is the fact that, over time, various governments have chipped away at Nova Scotians' access and privacy rights by creating exemptions and notwithstanding provisions sprinkled across numerous other pieces of legislation. This repeal by degrees has diluted access to information rights, slowly weakening legislation essential to the health of the province's democracy.

I recommend improvements in three core areas:

- Draft one comprehensive law that covers all public bodies and municipal bodies currently subject to the various access laws.
- Review all exemptions and notwithstanding clauses with a view to reducing them to a minimum using a set of pre-determined criteria.
- Subject Members of the Legislative Assembly (MLA) offices and all officers of the legislature to the privacy rules under the new law.

Summary of Recommendations

Organization and Coverage

Recommendation #1: Organization of the Acts
Combine the access and privacy rules contained in the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*), *Municipal Government Act Part XX* (*MGA*), *Personal Information International Disclosure Protection Act* (*PIIDPA*), and *Privacy Review Officer Act* (*PRO*) into one complete *Freedom of Information and Protection of Privacy Act.*

Recommendation #2: Extending coverage
a) Create a clear, criteria-based definition of public body.
b) Make MLA offices and officers of the legislature subject to the privacy rules set out in *FOIPOP*.

Recommendation #3: Conflict with other enactments
a) Conduct a thorough review of all of the conflict clauses listed in ss. 4A(2) of *FOIPOP* and 464A(2) of the *MGA* with a view to reducing the list to only those that are demonstrably necessary. The review should take into consideration the exemptions to disclosure already in existence and should particularly avoid unnecessary exclusions in light of the exemptions.
b) Require periodic statutory reviews of ss. 4A(2) of *FOIPOP* and 464A(2) of the *MGA*.
c) Add a provision to specify the criteria for when a notwithstanding clause would be appropriate in *FOIPOP* and the *MGA*.
d) Add a provision requiring government to list provisions in statutes that prevail over *FOIPOP* and the *MGA* in schedules to the Acts and include a review of these schedules in any regular review of *FOIPOP* or the *MGA*.

Modernizing Access Rights

Recommendation #4: Protecting applicant identity
Add a provision to Nova Scotia's access law requiring that the name of applicants be kept confidential except as specifically enumerated for the purposes of processing an access request or appeal related to that request.

Recommendation #5: Fees
a) Eliminate the $5 application fee.
b) Allow for a minimum of five hours of search and processing time before any fee is charged.
c) Prohibit charging of fees for time spent severing the record.
d) Impose timelines for decisions relating to fee waiver requests.
e) Add public interest as a ground for fee waivers by municipalities.
f) Require refund of fees when decisions are issued late.

Recommendation #6: Format of records
Amend s. 8(2) of *FOIPOP* and s. 468(2) of the *MGA* to specify that when a record is in electronic form, the head shall give access to the record in an open, reusable and accessible format.

Recommendation #7: Time
a) Require public bodies and municipalities to respond to correction requests within 30 days.
b) Amend s. 9 of *FOIPOP* and s. 469 of the *MGA* to permit public bodies and municipalities to take a time extension of up to 30 days with the consent of the applicant.
c) Impose timelines for decisions related to fee waiver requests (consistent with recommendation #5(d) above).

Recommendation #8: Modernizing exemptions

a) Place a time limit on each exemption.
b) Exclude business contact information from the definition of personal information.

Recommendation #9: Duty to document

Create a legislated duty to document in *FOIPOP* and the *MGA*. Subject this duty to the oversight of the Commissioner.

Recommendation #10: Authorization to disregard requests

Add a provision to *FOIPOP* and the *MGA* that allows for public bodies and municipalities to disregard requests that would amount to an abuse of process with the permission of the Commissioner.

Recommendation #11: Open government

a) Amend *FOIPOP* to ensure that the Commissioner has oversight over public body compliance with the publication requirement set out in s. 48.
b) Add a provision to *FOIPOP* requiring that the Minister responsible for the Act deliver an annual statistical report regarding government's performance to the House of Assembly. Require that the report be published within four months of year end.
c) Remove s. 48(7) and provide, at a minimum, that all government departments must comply with the publication requirement without a need for any further regulation.

Recommendation #12: Public interest override

a) Make the public interest override provision mandatory.
b) Add a new provision requiring public bodies and municipalities to always consider the public interest before exempting information under a discretionary exemption.

Modernizing Privacy Rights

Recommendation #13: Standards of sharing personal information

a) Repeal ss. 27(f) and 27(g) of *FOIPOP* and ss. 485(2)(f) and 485(2)(g) of the *MGA* and replace those provisions with provisions that permit disclosure within the public body or within the municipality where the information is necessary for the performance of the duties of the employee of or service provider to the public body or municipality.
b) Add new provisions that permit disclosure for the purposes of the delivery of a common or integrated program or service. Add a definition of common or integrated program or activity that requires documentation of the program and a privacy impact assessment. Require public bodies to notify the Commissioner as early as possible of any proposed common or integrated program or activity. Make privacy impact assessments mandatory for any common or integrated program or activity and require public bodies to provide a copy of the privacy impact assessment for comment by the Commissioner.
c) Add a new provision that permits disclosure of personal information to a provincial identity service provider. Authorize the Minister responsible for the Act to designate a public body as the provincial identity service provider and set out the permitted activities of such an entity. The amendments should include limitations on the collection of personal information by the provincial identity service provider.
d) Add a new provision that permits disclosure of personal information to a big data institute. Define the nature of the institute and require that it include privacy, human rights, and ethical expertise in data integration and analytics. Include a requirement for data minimization, mandatory privacy impact assessments to be provided to the Commissioner, and threat risk

assessments for all big data initiatives. Include these initiatives in the mandatory breach notification process.

Recommendation #14: Core privacy standards

Add three core privacy standards to *FOIPOP* and the *MGA*:

a) Prohibit collection, use, or disclosure of personal information if other information will serve the purpose.
b) Limit collection, use, and disclosure of personal information to the minimum personal information necessary.
c) Permit disclosure of personal information within an organization only on a need to know basis.

Recommendation #15: Privacy impact assessments

a) Require that public bodies and municipalities complete a privacy impact assessment on all new projects, programs, systems, enactments, and activities.
b) Require that public bodies that are government departments submit their privacy impact assessments to the Minister responsible for the Act for the Minister's review and comment.
c) Where the proposed program, project, system, or activity involves a common or integrated program or activity, require that the privacy impact assessment be provided to the Commissioner for comment (consistent with recommendation #12(b) above).
d) Where the proposed program, project, system, or activity involves big data, require that a privacy impact assessment be completed and provided to the Commissioner for comment (consistent with recommendation 13(d) above).

Recommendation #16: Information sharing agreements

a) Amend *FOIPOP* and the *MGA* to require that any regular sharing of personal information by public bodies or municipalities be in writing in the form of information sharing agreements. Include requirements regarding the content of the information sharing agreements.
b) Require public bodies and municipalities to notify the Commissioner of all new or amended agreements to share personal information and give the Commissioner explicit authority to review and comment on the agreements.
c) Require publication of the existence and nature of the information sharing agreements between public bodies, municipalities, and with other external bodies.

Recommendation #17: Privacy management program requirements

Add a requirement that public bodies and municipalities have a privacy management program that:

a) Designates one or more individuals to be responsible for ensuring that the public body or municipality complies with *FOIPOP* and the *MGA* from within the organization.
b) Is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body or municipality.
c) Includes policies and practices that are developed and followed so that the public body or municipality can meet its obligations under *FOIPOP* or the *MGA*, and makes policies publicly available.
d) Includes mandatory privacy training for all employees.
e) Has a process to respond to complaints that may arise respecting the application of *FOIPOP* or the *MGA*.
f) Is regularly monitored and updated.

Recommendation #18: Mandatory privacy breach notification

a) Require notification to affected individuals and the Commissioner, without unreasonable delay, of all privacy breaches involving a real risk of significant harm.
b) Specify content requirements for notification to individuals including: details about the cause of the breach, a list of the type of data lost or stolen, an explanation of the risks of harm affected individuals may experience as a result of the breach, and information about the right to complain to the Commissioner.
c) Authorize the Commissioner to order notification to an individual affected by the breach.
d) Require maintenance of a record of all data breaches with specified details available to the Commissioner upon request.

Recommendation #19: Mandatory consultation on draft legislation

a) Impose a duty on Ministers to consult with the Commissioner on any proposed Bill that could have implications for access to information or protection of privacy prior to introduction into the House.
b) Provide the Commissioner with the necessary general power to comment on the implications for access to information or for protection of privacy of proposed legislative schemes.

Recommendation #20: Collection notification

a) Add a requirement to *FOIPOP* and the *MGA* that personal information must be collected directly from the individual the information is about unless the law authorizes another method of collection.
b) Where information is collected directly from an individual, require that the public body or municipality tell the individual from whom it collects personal information the purpose for collecting it, the legal authority for collecting it, and the contact information of an individual who can answer any questions.

Recommendation #21: Personal information banks

a) Repeal s. 48(7) so that the requirement for personal information banks applies to all public bodies and without any further legislative effort (consistent with recommendation 11(c)).
b) Require that municipalities publish and maintain personal information banks.

Improving Oversight

Recommendation #22: Officer of the legislature

Make the Information and Privacy Commissioner (Review Officer and Privacy Review Officer) an officer of the legislature.

Recommendation #23: Name change

Change the name of the oversight body in *FOIPOP* with necessary consequential amendments to *PRO*, the *Personal Health Information Act* (*PHIA*) and the *MGA* to "Information and Privacy Commissioner".

Recommendation #24: Employees, experts, and support

a) Authorize the Commissioner to appoint employees she considers necessary in such positions she considers appropriate under such classification ratings and at such rates of remuneration within those classification ratings established by the Public Service Commissioner.
b) Authorize the Commissioner to engage the services of such counsel or other professionals or experts to advise or assist the Commissioner notwithstanding any government procurement rules or policies.
c) Authorize the Commissioner to delegate any of her powers except the power to delegate. Make clear that such delegation may occur when the Commissioner declares a conflict of interest.

Recommendation #25: Restrictions on disclosure and immunity

Add a provision enumerating the permitted uses and disclosures of information by the Commissioner and her staff and a provision specifying the immunity of the Commissioner and her staff.

Recommendation #26: Authority of the Commissioner

Amend *FOIPOP* and the *MGA* to shift the burden onto the public body or municipality to seek a declaration of the Nova Scotia Supreme Court whenever the public body or municipality decides that it will not follow the recommendations of the Commissioner.

Recommendation #27: Power to determine procedure

Amend s. 38 of *FOIPOP* and s. 491 of the *MGA* to add general powers of the Commissioner that include the power to determine the procedure to be followed in the exercise of the powers or performance of any duties pursuant to the *MGA* or *FOIPOP*.

Recommendation #28: Power to compel production

Amend s. 38 of *FOIPOP* to:

a) Make clear that solicitor-client privilege is not affected by disclosure to the Commissioner.
b) Require any person to produce a record for the Commissioner that is in the person's custody or control, including personal information.
c) Require the Commissioner to return any record or copy of any record produced by the public body concerned.

Recommendation #29: Information sharing between oversight agencies

Amend *FOIPOP* and the *MGA* to allow the Commissioner to exchange information with extra-provincial Commissioners for the purpose of coordinating activities and handling reviews and complaints involving two or more jurisdictions.

Recommendation #30: Grounds to refuse to proceed with a review

a) Amend *FOIPOP* and the *MGA* to add a provision that states that where the Commissioner is satisfied that there are reasonable grounds to review any matter, the Commissioner shall review the matter. Include grounds where the Commissioner may refuse to conduct a review including where the application is frivolous or vexatious, not made in good faith, concerns a trivial matter, does not contain sufficient evidence, has already been the subject of a report by the Commissioner, the public body has responded adequately to the complaint, the length of time that has elapsed, or for any other reason it is fair and reasonable not to conduct a review.
b) Amend s. 39 of *FOIPOP* and s. 492 of the *MGA* to provide that on completing a review the Commissioner "may" prepare a written report rather than "shall" prepare a written report.

Recommendation #31: Review and complaint time limits
Amend *FOIPOP* and the *MGA* to provide that the Commissioner should conclude her investigation and mediation processes and, if necessary, issue a report within 90 days of receipt of a complaint or request for review. Include an option to allow for longer period of time at the Commissioner's discretion and with written notice to the parties.

Recommendation # 32: General powers of Commissioner
Amend s. 38 of *FOIPOP* and s. 491 of the *MGA* to add general powers of the Commissioner that include the following:

a) Monitor how the privacy and access provisions are administered and conduct reviews of access and privacy complaints arising from the access and privacy provisions.
b) Initiate investigations of access and privacy compliance including matters or allegations of unauthorized destruction of records.
c) Make recommendations on and mediate access and privacy complaints.
d) Undertake research matters concerning privacy and access legislation.
e) Inform the public about the Acts.
f) Conduct audits.
g) Authorize public bodies and municipalities to disregard requests.
h) Determine OIPC procedures.
i) Comment on the implications for access to information or for protection of privacy of any matter including proposed projects, activities, systems, information sharing agreements and legislative schemes of public bodies and municipal bodies.

Offences

Recommendation #33: Update offence provisions
Update Nova Scotia's offence provisions by:

a) Making the following offences under the law:
   - obstructing the Commissioner;
   - misleading the Commissioner and knowingly making a false statement to the Commissioner;
   - obstructing the right of access by destroying, altering, falsifying, or concealing a record with intent to evade a request for access;
   - directing another to destroy, alter, falsify, or conceal any record; and
   - willfully or knowingly collecting, using, or disclosing personal information in contravention of the law.
b) Set the fine on conviction at a maximum of $20,000 for individuals and higher for organizations and service providers.

Review of the Acts

Recommendation #34: Review of the Acts
Amend s. 50 of *FOIPOP* and add provisions to *PRO*, *PIIDPA* and the *MGA* to require that:

a) A review must be conducted of each Act at least every six years.
b) The reviews must be conducted by an independent committee of the legislature.
c) All submissions and reports of the committee must be made public.
d) Each review must include a mandatory review of any and all notwithstanding clauses and a review of s. 4A(2) of *FOIPOP* and s. 464A(2) of the *MGA*.

Table of Contents

A. Introduction – Why Now?

History

Nova Scotia is proud of the fact that it had the first provincial access law that came into effect in 1977. Nova Scotia's "modern" access law was written in 1993 and came into effect in 1994 – more than 20 years ago. The world has changed dramatically in that time, particularly the world of information. In 1993 there were 130 websites, today there are 1 billion. We used VCR's to record television programs and cell phones only made phone calls. Google wasn't founded until 1998 and Facebook wasn't created until 2004. Big data was the realm of scientists and dreamers.

The *Freedom of Information and Protection of Privacy Act* (*FOIPOP*) is the foundational access and privacy law in Nova Scotia. The *Municipal Government Act* (*MGA*) version of the *FOIPOP* rules, which are virtually identical, came into effect in 1999 and Nova Scotia's privacy oversight rules came into effect with the enactment of the *Privacy Review Officer Act* (*PRO*) in 2009.

FOIPOP has been amended 17 times since it came into effect. Fourteen of those amendments related to either adding or removing an enactment from the list of legislation that prevails over *FOIPOP*, or adding, removing or renaming entities identified in *FOIPOP*. Two amendments related to adjusting the fee structure. Only the 1999 amendments were substantial – bringing local public bodies under *FOIPOP*, adding the conflict with other enactments provision, refining the third party notice provisions and updating the powers of the Information and Privacy Commissioner (called "review officer" in *FOIPOP* and the *MGA*).[1]

FOIPOP, in its current form, has had only one statutory review by a special advisory committee to the Minister of Justice. Its report was submitted in October 2003,[2] and resulted in only a few small changes to the fees under *FOIPOP*. Interestingly, many of the recommended updates to *FOIPOP* made by the committee in 2003 remain relevant today and are discussed below including: the need for a power to disregard frivolous and vexatious requests, giving the Commissioner powers to initiate access investigations, providing the Commissioner with more resources to mediate disputes, and updating privacy protections.

An international non-governmental agency, the Centre for Law and Democracy, has developed a rating system that evaluates the strength of access to information legislation around the world. Mexico currently has the highest mark of 136 and Austria currently has the lowest mark of 32. Nova Scotia's access law earned a mark of 85, making it 7th in Canada and 56th in the world – the same position as Rwanda and Italy. Newfoundland and Prince Edward Island's laws both rank higher than Nova Scotia's. New Brunswick's law earned a mark of 79, the lowest mark given for a Canadian jurisdiction.

[1] Effective September 2015, we began referring to the FOIPOP Review Office as the Office of the Information and Privacy Commissioner and the Review Officer and Privacy Review Officer as the Information and Privacy Commissioner. I will use those terms throughout the report. No legislative change was made and so *FOIPOP*, *PRO* and the *MGA* use the old titles of Review Officer and Privacy Review Officer.

[2] The Freedom of Information and Protection of Privacy Act: Advisory Committee Special Report, Submitted to the Minister of Justice October 24, 2003 available at: https://www.novascotia.ca/just/IAP/review/_docs/foipopreviewreportoct24.pdf.

Recent Developments

Six provinces,[3] two territories, and the federal government have recently undertaken reviews of or updates to their public sector access laws. Many of the ideas in this report can be found in reports from these other jurisdictions. Citizens and governments have become increasingly aware of the need to modernize access and privacy laws to ensure that they continue to enshrine meaningful and enforceable rights. Most importantly, the laws need to adapt so that they can continue to serve their original purposes of these laws that remain relevant today.

Nova Scotia public bodies and municipalities want and need to take advantage of modern technologies to deliver services to citizens. Citizens expect this type of service. But with technology comes both opportunity and risk. Risk to privacy and access rights. A thorough review and update of our laws will help us manage these risks while ensuring that our fundamental rights remain protected.

[3] Attached as Appendix 2 to this document is a list of the recent reviews conducted in Alberta, British Columbia, Canada, Newfoundland, New Brunswick, Northwest Territories, Quebec, Saskatchewan, and the Yukon.

B. Organization and Coverage

i. Organization of the Acts
ii. Extending Coverage
iii. Conflict with Other Enactments

B. i Organization of the Acts

Problem

Nova Scotia has a confusing array of access and privacy laws.[4] There are currently four access and privacy laws that apply to a greater or lesser extent to all public bodies and municipalities in Nova Scotia:

- *Freedom of Information and Protection of Privacy Act* (*FOIPOP*)
- *Municipal Government Act, Part XX* (*MGA*)
- *Privacy Review Officer Act* (*PRO*)
- *Personal Information International Disclosure Protection Act* (*PIIDPA*)

The rules in these four laws could easily be combined into one law, as a complete code of the access and privacy rules that apply to public bodies and municipalities. Such an approach would be consistent with virtually every other jurisdiction in Canada. It would also ensure that municipalities and public bodies are subject to the same access and privacy standards – something citizens rightly expect.

As a result of having the rules scattered across these various statutes a number of inconsistencies arise. First, although the *MGA* access and privacy rules are essentially the same as the *FOIPOP* rules, because the privacy oversight powers of the Commissioner are set out in a third Act, the *Privacy Review Officer Act,* municipal bodies, including police, are subject to privacy rules but are not subject to any privacy oversight. In other words, when citizens' privacy rights are violated by municipalities or police, there is no complaint mechanism in the law.

A second anomaly is that rules regarding disclosures of personal information outside of Canada were placed in a separate law from the *Freedom of Information and Protection of Privacy Act*. That law, the *Personal Information International Disclosure Protection Act*, has no independent oversight requirements. Therefore, when a citizen's personal information is accessed or disclosed outside of Canada and the public body claims such disclosure is authorized under *PIIDPA*, the affected citizen has no right to complain to the Information and Privacy Commissioner. There is no independent oversight mechanism in *PIIDPA*.

Nova Scotia is a small jurisdiction. Having four separate access and privacy laws does not make sense to citizens. Their expectations with respect to their rights to access information or to protection of their personal information is the same no matter what level of government has the information. One streamlined consistent law for all government bodies would be more accessible and comprehensible for citizens and the public bodies themselves.

[4] In addition to the four access and privacy laws cited here, Nova Scotia also has an access and privacy law for personal health information – the *Personal Health Information Act* (*PHIA*). *PHIA* came into effect on June 1, 2013 and is currently undergoing a legislative review. It is not the subject of this report but I have made reference to some of the more modern provisions found in *PHIA* that could be adapted to *FOIPOP* or the *MGA*.

Other Jurisdictions
The usual approach in Canada is that all public bodies are covered by one comprehensive access and privacy law. The full scope of coverage varies between jurisdictions but all bodies covered are subject to access and privacy oversight of an Information and Privacy Commissioner. In addition, Nova Scotia is the only jurisdiction that has a separate law for disclosures of personal information outside of Canada.

Jurisdictions with a single law for all enumerated public bodies are listed below. Each of these laws includes independent oversight of access and privacy rules by a Commissioner and includes rules for the access, storage or disclosure of personal information outside of Canada:

> **Newfoundland**: *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2
> **Prince Edward Island:** *Freedom of Information and Protection of Privacy Act*, c. F15-01
> **New Brunswick**: *Right to Information and Protection of Privacy Act*, S.N.B. 2009, c. R-10.6
> **Manitoba**: *Freedom of Information and Protection of Privacy Act*, C.C.S.M. c. F. 175
> **Alberta:** *Freedom of Information and Protection of Privacy Act*, RSA 2000 c. F-25
> **British Columbia**: *Freedom of Information and Protection of Privacy Act* RSBC c. 165
> **Yukon:** *Access to Information and Protection of Privacy Act*, RSY 2002, c. 1
> **Northwest Territories:** *Access to Information and Protection of Privacy Act,* S.N.W.T. 1994, c. 20

There are two exceptions to this approach: Saskatchewan and Ontario. Both have freedom of information laws specifically for municipal bodies. However, both laws include the full suite of privacy protections and full oversight by an Information and Privacy Commissioner. Further, both laws include the rules regarding access, storage and disclosure of personal information outside of Canada.

> **Saskatchewan:** *The Local Freedom of Information and Protection of Privacy Act*, S.S. 1990-1992, Chapter L-27.1
> **Ontario:** *Municipal Freedom of Information and Protection of Privacy Act*, R.S.O. 1990 c. M. 56

Recommendation #1: Organization of the Acts
Combine the access and privacy rules contained in the *Freedom of Information and Protection of Privacy Act* (*FOIPOP*), *Municipal Government Act Part XX* (*MGA*), *Personal Information International Disclosure Protection Act* (*PIIDPA*), and *Privacy Review Officer Act* (*PRO*) into one complete *Freedom of Information and Protection of Privacy Act.*

I will now address individual issues within the access and privacy laws. While each of the following recommendations addresses changes to *FOIPOP* and the *MGA*, each recommendation could simply be incorporated into one comprehensive law.

B. ii Extending Coverage

Problem

Currently *FOIPOP* applies to any "public body". "Public body" is defined in *FOIPOP* s. 3(1)(j). The definition is highly technical and confusing. It includes undefined terms such as "servants of the Crown". It is also inconsistent with the definition of "public body" found in the *Government Records Act*.[5] *FOIPOP* could be improved by more clearly identify criteria for when a body should be covered by the law.

In addition, several bodies, including officers of the legislature, are excluded from coverage under the Act. It appears that the original intent of this exclusion was to ensure that these offices could control access to information in their custody or control. This is typical of many Canadian jurisdictions. But officers of the legislature often have highly sensitive personal information in their possession. There is no public policy reason why those offices should not be subject to the privacy protection rules set out in the law.

MLA offices are funded by taxpayers. MLA's serve the public and in that capacity their offices often collect highly sensitive personal information of constituents seeking assistance from their MLAs. Subjecting MLA offices to the privacy rules under *FOIPOP* would ensure that this data is properly collected, used, disclosed and secured.

Other Jurisdictions

In 2015, the Information Commissioner of Canada provided a special report to Parliament entitled, *Striking the Right Balance for Transparency: Recommendations to modernize the Access to Information Act*.[6] In that report the Information Commissioner states that various model laws recommend a criteria based approach to defining coverage under the law. The relevant criteria include: whether the entity was established by statute, whether it receives substantial government funding, or whether it carries out public functions or services.

Two other jurisdictions in Canada have recently considered the application of the law to MLA offices and to officers of the legislature. Saskatchewan currently has a bill at second reading that

---

[5] SNS 1995-96, c 7; s. (3)(f) "public body" means a Government department or a board, commission, committee, office, foundation, agency, tribunal, task force, council, association or other body of persons, whether incorporated or unincorporated, all the members of which or all the members of the board of management or board of directors of which

> (i) are appointed by order of the Governor in Council, or
> (ii) if not so appointed or specified, in the discharge of their duties are public officers or servants of Her Majesty in right of the Province, but does not include the House of Assembly, its committees, the House of Assembly Management Commissioner, the Office of the Speaker, the Office of the Clerk of the House the Office of the Legislative Counsel, the Office of the Conflict of Interest Commissioner, the caucus offices, the offices of party leaders or any other offices within the jurisdiction of the House of Assembly or the Speaker and, for greater certainty, does include
> (iii) the Office of the Auditor General,
> (iv) Elections Nova Scotia, and
> (v) the Office of the Ombudsman,

and includes a public body designated as a public body pursuant to clause 14(1)(c).

[6] Information Commissioner of Canada, *Striking the Right Balance for Transparency - Recommendations to modernize the Access to Information Act*: http://www.oic-ci.gc.ca/eng/rapport-de-modernisation-modernization-report.aspx.

includes a number of amendments to its *Freedom of Information and Protection of Privacy Act.*[7] Included in the amendments is a change in the scope of the coverage of the Act that subject MLA offices to the privacy rules under the privacy law.

By way of contrast, Newfoundland's new access law continues to exempt constituency offices from access and privacy rules but does subject statutory offices to both access and privacy rules.

A third jurisdiction, British Columbia, has for some time had privacy laws that apply to officers of the legislature and to MLA offices. MLA offices are exempt from the public sector privacy law by virtue of the definition of "public body" in Schedule 1 to the BC *Freedom of Information and Protection of Privacy Act*. However, MLA offices are subject to the private sector privacy law as they fall within the broad definition of "organization" within the *Personal Information Protection Act* (PIPA). PIPA's application to MLA's records is limited to employee information.

Officers of the legislature are also exempt from the access provisions of British Columbia's public sector law but are subject to certain enumerated privacy rules including the requirement to protect personal information, the limitations on storage and access outside of Canada and the limitations on collection, use, and disclosure of personal information that apply to all public bodies.

Recommendation #2: Extending coverage
a) Create a clear, criteria-based definition of public body.
b) Make MLA offices and officers of the legislature subject to the privacy rules set out in *FOIPOP*.

B. iii Conflict with Other Enactments

Problem
Section 4A(2) of *FOIPOP* and s. 464A(2) of the *MGA* list enactments that restrict or prohibit access to any record and that prevail over *FOIPOP* or the *MGA*. This list has been amended from time to time and currently consists of 20 Acts that prevail over the *MGA* and 21 over *FOIPOP*. None of these provisions were subject to review by the Information and Privacy Commissioner, nor were any of them subject to a privacy impact assessment.[8] This means that individually, none of these conflict clauses received a thorough independent review with respect to the implications for the access and privacy rights of citizens. More troubling is the fact that the entire list has not been the subject of any review.

Other Jurisdictions
In 2015, when a special committee reviewed Newfoundland's access to information law, it focused particularly on the Newfoundland provision similar to s. 4A(2) of Nova Scotia's law. Following its review, the committee recommended two things relevant to this discussion. First, after conducting a review of each of the listed provisions, the committee recommended the removal of a number of

[7] Bill No. 30: *An Act to Amend the Freedom of Information and Protection of Privacy Act 2016*, available at: http://docs.legassembly.sk.ca/legdocs/Bills/28L1S/Bill28-30.pdf.
[8] There is no requirement that draft legislation be subject to a privacy impact assessment and no privacy impact assessments of draft legislation have ever been provided to the Office of the Information and Privacy Commissioner.

the provisions that prevail over Newfoundland's access law. Second, the committee recommended that the list be subject to regular reviews in order to assess the justification for the provisions.[9]

Recommendation #3: Conflict with other enactments

a) Conduct a thorough review of all of the conflict clauses listed in ss. 4A(2) of *FOIPOP* and 464A(2) of the *MGA* with a view to reducing the list to only those that are demonstrably necessary. The review should take into consideration the exemptions to disclosure already in existence and should particularly avoid unnecessary exclusions in light of the exemptions.
b) Require periodic statutory reviews of ss. 4A(2) of *FOIPOP* and 464A(2) of the *MGA*.
c) Add a provision to specify the criteria for when a notwithstanding clause would be appropriate in *FOIPOP* and the *MGA*.
d) Add a provision requiring government to list provisions in statutes that prevail over *FOIPOP* and the *MGA* in schedules to the Acts and include a review of these schedules in any regular review of *FOIPOP* or the *MGA*.

[9] Recommendations 37 and 41 found in the *Report of the 2014 Statutory Review of the Access to Information and Protection of Privacy Act Newfoundland and Labrador,* March 2015: http://www.ope.gov.nl.ca/publications/pdf/ATIPPA_Report_Vol2.pdf.

C. Modernizing Access Rights

i. Protecting Applicant Identity
ii. Fees
iii. Format of Records
iv. Time
v. Modernizing Exemptions
vi. Duty to Document
vii. Disregarding a Request
viii. Open Data & Open Government
ix. Mandatory Public Interest Override

C. i Protecting Applicant Identity

Problem
The identity of access to information applicants is personal information protected by the privacy rules in *FOIPOP* and the *MGA*. Unfortunately, many smaller public bodies and municipal bodies in Nova Scotia are not always aware that applicant information is protected and cannot be disclosed even within a public body unless authorized under the law. Instead, applicant identities may be commonly known by staff other than the access coordinator and sometimes, at the municipal level, by council members. Except where an individual seeks a copy of his or her own personal information, the identity of the applicant is irrelevant to whether or not exemptions to disclosure may apply to the record. Decisions about what can and cannot be disclosed must be made based only on the limited and specific exemptions set out in the law. This is the only way to ensure that applicants are treated fairly and that public bodies and municipalities are open and accountable.

Other Jurisdictions
Newfoundland's new law directly addresses this issue by requiring that the head of the public body ensures that the identity of an applicant is only disclosed to employees responsible for the processing of access requests and the Commissioner.

Recommendation #4: Protecting applicant identity
Add a provision to Nova Scotia's access law requiring that the name of applicants be kept confidential except as specifically enumerated for the purposes of processing an access request or appeal related to that request.

C. ii Fees

Problem
Fees create a barrier to access. But fees also partially compensate government for the costs associated with the processing of access requests. The process of retrieving responsive records and then reviewing them to determine if any exemptions apply is labour intensive and can take many hours to complete. The question is, should all taxpayers bear the costs associated with all access to information requests?

Nova Scotia's laws require applicants to pay an initial $5 application fee and then further fees at $30 per hour for costs associated with processing the requests, although the first two hours of time to locate and retrieve a record is free. Individuals seeking copies of their own personal information are not required to pay any fees. The law currently permits applicants to ask public bodies to waive

fees.[10] The fee waiver provisions in *FOIPOP* and the *MGA* are not consistent. The *MGA* fails to specifically allow for fee waivers in the public interest.

This office investigates complaints relating to fees. Those complaints are on the rise. In 2013, and again in 2014, fee complaints made up only 4% of our caseload. In 2015/2016, fee complaints made up 5% of our much larger caseload.[11]

Another concerning pattern is the government's own statistics show that the amount of fees charged is on the rise. In 2013, government departments reported that they had charged a total of $10,683 in fees for the processing of access requests. In its most recent annual report, the Government of Nova Scotia reported that departments had charged $32,278. This is a 202% increase in fees at a time when the number of access requests only increased 26%. Put another way, the average cost of a *FOIPOP* request to a government department in 2013 was $8.25 and in 2015/16 it was $14.13 per request.[12]

Our experience reveals a number of concerns with respect to fees. First, the $5 application fee is so low as to not be meaningful in terms of revenue to the government. The processing costs for a $5 payment is likely significantly greater than $5. There is no cost-recovery value of continuing to charge this fee. This means that the only purpose this fee serves is to place a barrier to access for applicants who cannot afford to pay.

Second, the fee process delays the processing of access requests. In essence, the law allows the public body or municipality to put the request "on hold" pending the outcome of the fee process. It is inconsistent with the purposes of the Acts to allow public bodies and municipalities to hold up access to information for unspecified periods of time while considering whether to waive fees.

Two other issues are also apparent from our investigations. We frequently find that higher fees are associated with poor records management and public bodies and municipalities do not have a good understanding of when to waive fees in the public interest.

Other Jurisdictions

Application fees:

Aside from Nova Scotia, only Ontario, Alberta, and PEI laws require payment of an application fee. By contrast there are no applications fees in any other Canadian province, nor are there application fees in Australia, New Zealand, or the U.K.[13]

[10] *FOIPOP* s. 11(7)(a), *MGA* s. 471(7).

[11] Our annual reports list the types of complaints received by file type. These reports are available on our website at foipop.ns.ca.

[12] Government provides annual statistics relating to its processing of access to information requests. The 2013 statistics are taken from the 2014 statistical report. The 2015/16 statistics are available at: http://novascotia.ca/is/reports/FOIPOP-Annual-Report-2015-2016.pdf. In 2013 government departments received 1679 new access requests and collected $10,683 in fees = $8.25 per request. In 2015/16 government departments received 2285 new access requests and collected $32,278 in fees = $14.13 per request.

[13] As summarized by Suzanne Legault, the Information Commissioner of Canada, in *Striking the Right Balance for Transparency: Recommendations to modernize the Access to Information Act,* March 2015 available at: http://www.oic-ci.gc.ca/eng/rapport-de-modernisation-modernization-report.aspx at p. 21, n 27.

Free processing time:

The amount of free processing time varies between jurisdictions in Canada. The greatest amount of free time is granted under Newfoundland's new law: 10 to 15 hours. Other jurisdictions allow for the following amounts of free time:

2 hours – Nova Scotia, Saskatchewan,[14] Manitoba,[15] Prince Edward Island[16]
3 hours – British Columbia[17]
5 hours – Canada – in practice by virtue of a recent policy directive, all fees other than the application fee are currently being waived at the federal level[18]
10-15 hours – Newfoundland (discussed below)
No fee for time spent reviewing records – Alberta[19]
No fee for time spent to sever records – British Columbia[20]

The Newfoundland law goes on to permit fee waivers for financial hardship or when it would be in the public interest to disclose the record.

In her review of the *Access to Information Act* published in 2015, Canada's Information Commissioner, Suzanne Legault, examined the fee regime under that law.[21] She noted that the law requires a $5 application fee and permits fees for every hour after the first five hours for search and preparation of records for release. She notes that determining fee amounts and processing fee payments adds complexity to the administration of access requests and results in delays for requesters. Fees are also inconsistently applied across institutions according to Commissioner Legault. Fees related to search times in particular depend on the quality and implementation of information management practices. She concludes by recommending that all fees be eliminated.

In May 2016, the federal government issued a policy directive that government departments were required to waive all access application fees apart from the initial $5 application fee.[22]

---

[14] *Freedom of Information and Protection of Privacy Regulation* 101/2007 as amended, s. 6(2), available at http://www.qp.gov.sk.ca/documents/English/Regulations/Regulations/F22-01R1.pdf.

[15] *Access and Privacy Regulation,* 64/98, s. 4(2) available at: http://web2.gov.mb.ca/laws/regs/current/_pdf-regs.php?reg=64/98.

[16] *Freedom of Information and Protection of Privacy Act General Regulations*, s. 9(4) available at: https://www.princeedwardisland.ca/sites/default/files/legislation/f15-01g_0.pdf.

[17] *Freedom of Information and Protection of Privacy Act*, R.S.B.C. c. 165, s. 75(2)(a).

[18] *Access to Information Act*, R.S.C. 1985, c. A.1. Treasury Board directive that heads will waive all fees other than the application fee is available at: https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310.

[19] The details of Alberta's fee structure are set out in the *Freedom of Information and Protection of Privacy Regulation* 186/2008. Section 11(6) of that Regulation provides that a fee may not be charged for time spent reviewing a record. The Regulation is available at: http://www.qp.alberta.ca/documents/Regs/2008_186.pdf.

[20] *Freedom of Information and Protection of Privacy Act*, R.S.B.C. c. 165, s. 75(2)(b).

[21] Information Commissioner of Canada, *Striking the Right Balance for Transparency: Recommendations to modernize the Access to Information Act,* March 2015 available at: http://www.oic-ci.gc.ca/eng/rapport-de-modernisation-modernization-report.aspx.

[22] Treasury Board of Canada Secretariat, "Interim Directive on the Access to Information Act" available at: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18310&utm_source=referral&utm_medium=news&utm_term=canada&utm_content=directive&utm_campaign=interimati.

Recommendation #5: Fees

a) Eliminate the $5 application fee.
b) Allow for a minimum of five hours of search and processing time before any fee is charged.
c) Prohibit charging of fees for time spent severing the record.
d) Impose timelines for decisions relating to fee waiver requests.
e) Add public interest as a ground for fee waivers by municipalities.
f) Require refund of fees when decisions are issued late.

C. iii Format of Records

Problem

Public bodies and municipalities can be reluctant to provide citizens with access to information in electronic format. They raise concerns about manipulation of the data or reuse or potential misinterpretation of the data. But the foundation of access law, and one of its key benefits is that it places no limitation on the further use or disclosure of information accessed under the law. This makes perfect sense in light of the purposes for the Act: to facilitate informed public participation in policy formulation and to permit the airing and reconciliation of divergent views. What better way to accomplish this purpose than to publish information you have received in response to an access request? Divergent views cannot be reconciled until they are expressed – perhaps in the form of manipulated data to support a point of view.

In addition, while paper isn't exactly a thing of the past, it is also true that the vast majority of citizens now generally access information online. They interact with that information, manipulate it, repost it, tweet it, make memes out of it. Meaningful access means providing information to citizens in a reusable format. Nova Scotia's access law currently only permits applicants to either request a copy or request to examine the record. While the Act contemplates requests for access to information "stored by electronic or other technological means" it does not clearly provide for the right to receive information in electronic format.

Other Jurisdictions

Newfoundland's new law makes clear that individuals have the right to receive copies of records electronically where the record is in electronic form.[23]

Canada's federal Information Commissioner's recommendations to modernize the federal *Access to Information Act* in 2015 included a recommendation that public bodies be required to provide information to applicants in an open, reusable and accessible format by default unless the requester asks otherwise, it would cause undue hardship to the institution, or it is technologically impossible.[24] Commissioner Legault points out that the foundation for such a recommendation is found in open government principles. Those principles state that information should be provided to the public in open formats that facilitate reuse.[25]

Saskatchewan's recent proposed amendments in Bill 30 include a new provision mandating disclosure of electronic information in electronic form.[26]

---

[23] See Appendix 1 for a copy of the Newfoundland provision.
[24] *Striking the Right Balance for Transparency* at p. 20.
[25] Open Government Partnership, Open Government Declaration, September 2011 at http://www.opengovpartnership.org/about/open-government-declaration
[26] See Appendix 1 for a copy of the Saskatchewan provision.

Recommendation #6: Format of records
Amend s. 8(2) of *FOIPOP* and s. 468(2) of the *MGA* to specify that when a record is in electronic form, the head shall give access to the record in an open, reusable and accessible format.

C. iv Time

Problem
There are three essential time rules missing from our law. There is no time limit for how long a public body or municipality can take to respond to a correction request under s. 25 of *FOIPOP* or s. 484 of the *MGA*. There is no provision to allow a public body or municipality to take a time extension with the consent of the applicant. As noted earlier, there is no time limit for fee waiver decision. There are additional time issues in relation to exemptions and to the review process. I have discussed those time issues in sections specific to exemptions and to the Commissioner's processes.

Other Jurisdictions
The typical time limit for responding to correction requests in other jurisdictions is 30 days.[27]

An example of a provision permitted an extension of time with the consent of the applicant can be found in British Columbia's law and requires simply that the applicant consent, in the prescribed manner, to the extension.[28]

Recommendation #7: Time
a) Require public bodies and municipalities to respond to correction requests within 30 days.
b) Amend s. 9 of *FOIPOP* and s. 469 of the *MGA* to permit public bodies and municipalities to take a time extension of up to 30 days with the consent of the applicant.
c) Impose timelines for decisions related to fee waiver requests (consistent with recommendation #5(d) above).

C. v Modernizing Exemptions

Problem
Nova Scotia's exemptions to disclosure, set out in ss. 12 – 21 of *FOIPOP* and ss. 472 – 481 of the *MGA,* are similar to exemptions found in every other access law in Canada. But recent developments in other jurisdictions and concerns raised in Nova Scotia highlight the need for change in a two areas.

Time limits:
First, many of the exemptions do not have a time limit on them. Time limits create certainty in access laws. As soon as the time limit is reached or a specified event (such as publication) takes place, public bodies and municipalities would no longer be able to invoke the exemption to withhold the information.[29] In Nova Scotia the following time limits apply:

[27] See Alberta's *Freedom of Information and Protection of Privacy Act* R.S.A. 200, chapter F-25, s. 36(7).
[28] See British Columbia's *Freedom of Information and Protection of Privacy Act* R.S.B.C. 1995, c. 165, s. 10(1)(d).
[29] The Information Commissioner of Canada made a similar point in *Striking the Right Balance for Transparency* at p. 39.

Intergovernmental affairs	15 or more years
Deliberations of executive council	10 or more years
Advice to public body or Minister	5 or more years
Law enforcement	No time limit
Solicitor-client privilege	No time limit
Financial or economic interests of public body	No time limit
Health and safety	No time limit
Conservation	No time limit
Closed meeting of local public bodies	More than 15 years
Academic research	No time limit
University appointment related personal information	No time limit
Labour conciliation records	No time limit
Personal information	No time limit
Confidential third party business information	No time limit

Various time limits are applied to exemptions in other jurisdictions. Newfoundland's recently updated law includes a 50 year time limit for labour conciliation type records and a 50 year time limit for third party confidential business information.[30] The law also specifically states that the length of time a person has been deceased is a relevant consideration in determining whether or not the disclosure of the deceased person's personal information would be an unreasonable invasion of personal privacy.[31]

Canada's Information Commissioner has recommended that solicitor-client privilege be subject to a 12 year time limit after the last administrative action on the file.[32] The Commissioner points out that, "…the government's mandate is to pursue the public interest. This public interest aspect of government administration justifies differences in the operation of solicitor-client privilege. The government's public interest mandate provides heightened incentive to waive privilege to ensure greater transparency and accountability. Therefore, factors such as whether the protection is still relevant, whether the advice is old and outdated, or the historical value of the advice carry more weight in favour of disclosure."[33]

In his recent list of recommendations for the five year review of Quebec's access law, the President recommends that all restrictions set out in the Act respecting access be limited in duration.[34]

Business contact information:
Nova Scotian public bodies and municipalities frequently conduct business with third parties. Those third parties are represented by individuals who communicate with the public bodies on matters relating to the service or goods provided. In that context their names and business contact information does not raise any serious privacy issues. Usually the individuals identified are listed on company websites. The fact that they are providing services to public or municipal bodies is information important to citizens and important to ensuring transparency in government decision making. The test in both the *MGA* and *FOIPOP* is that disclosure should not result in an "unreasonable invasion of personal privacy." Despite the strictly business context in which this information appears, there is a strong tradition among Nova Scotian public bodies of severing third

[30] *Access to Information and Protection of Privacy Act*, 2015, SNL 2015 Chapter A-1.2 s. 38(2), s. 39(2).
[31] *Access to Information and Protection of Privacy Act*, 2015, SNL 2015 Chapter A-1.2 s. 40(5)(j).
[32] *Striking the Right Balance for Transparency* at p. 58.
[33] *Striking the Right Balance for Transparency* at p. 57.
[34] Commission d'acces a l'information du Quebec, *List of Recommendations in the Five-Year Report for 2016* p. 1.

party employee names and contact information (business name, phone numbers, business email addresses, and the address of the business). Other jurisdictions have made this a non-issue by adding an exception to the definition of "personal information" to exclude business contact information including name, position, business email, phone and address.

The Government of the Northwest Territories just completed a public consultation as part of its comprehensive review of the *Access to Information Act*. The report of those consultations noted that a majority of respondents supported removing business contact information from the definition of personal information.[35]

Recommendation #8: Modernizing exemptions
a) Place a time limit on each exemption.
b) Exclude business contact information from the definition of personal information.

C. vi Duty to Document

Problem
Nova Scotia does not have a statutory duty to document. This is an important issue from an access to information perspective because if records are not created documenting decisions, actions and deliberations, there are no records to access. The right to access government information and to therefore hold government to account is rendered meaningless.

The only requirements to document in Nova Scotia are set out in policy. Chapter 4 of the Common Service Manual states that "Business activities will be documented and any necessary audit trails will be built into systems and programs." There is no explanation of the scope and nature of what must be documented; there is no independent oversight of compliance with this requirement and no consequence for a failure to comply with the requirement. Departments simply monitor themselves.

The Government of Nova Scotia reports statistics on its access to information program. One of the statistics it reports is the outcome of access requests. Was full disclosure granted, partial disclosure granted or were no responsive records found? Between 2006 and 2011 no records responses occurred in response to an average of 14% of requests per year. From 2012 onward that average jumped to 29%. This is an extraordinary increase that suggests that lack of documentation could be a systemic problem.[36]

Other Jurisdictions
Jurisdictions around the world have been re-evaluating government obligations to document. Information and Privacy Commissioners in Canada have jointly called on all Canadian jurisdictions

[35] Government of Northwest Territories, *What we Heard: Results of the Public and Stakeholder Engagement on the Comprehensive review of the Access to Information and Protection of Privacy Act*, November 2016 at p. 8 available at: https://www.justice.gov.nt.ca/en/files/public-engagements-and-consultation-packages/What%20We%20Heard%20-%20Results%20of%20Public%20and%20Stakeholder%20Engagement%20Report%202016.pdf.
[36] Government officials have suggested that at least part of this increase may be attributable to the practice of real estate lawyers seeking access to any existing environmental certificates relating to properties. Such documents may or may not exist but it is the practice to always seek this confirmation during a real estate transaction. This would contribute to creating a high number of "no records exist" responses.

to create a legislated duty requiring all public entities to document matters related to deliberations, actions and decisions.[37]

Following the 2014 review of Newfoundland's access law, Newfoundland is in the process of creating a statutory duty to document although draft legislation is not currently available. The special committee examined issues regarding the reluctance of some governments to document because of fears of disclosure of the records through the access to information process. The evidence gathered by the special committee was sufficient for it to recommend that the government take the necessary steps to impose a duty to document.[38]

A recent legislative review in Ontario resulted in proposed amendments to create a statutory duty to document. The proposed amendments are to both the *Freedom of Information and Protection of Privacy Act* (s. 10.1) and to the *Municipal Freedom of Information and Protection of Privacy Act* (s. 4.1). They state:

> Every head of an institution shall ensure that reasonable measures respecting the records in the custody or under the control of the institution are developed, documented and put in place to preserve the records in accordance with any recordkeeping or records retention requirements, rules or policies, whether established under an Act or otherwise, that apply to the institution.

A new offence was also added to both laws providing that it is an offence to alter, conceal, or destroy a record or cause any other person to do so with the intention of denying a right under the law.

A Special Committee of the legislature recently completed its regular review of British Columbia's public sector access law. One of the eleven key recommendations of the committee was to add a duty to document. The Committee also recommended the creation of obligations related to ensuring a cohesive and robust information management scheme.[39] On March 8, 2017, the BC Government introduced Bill 6, Information Management (Documenting Government Decisions) Amendment Act, 2017 that included a proposed duty to document.

Recommendation #9: Duty to document
Create a legislated duty to document in *FOIPOP* and the *MGA*. Subject this duty to the oversight of the Commissioner.

---

[37] On March 1, 2016, Information and Privacy Commissioners from across Canada issued their most recent joint declaration on this topic available on the OIPC NS website at: https://foipop.ns.ca/sites/default/files/publications/Duty%20to%20Document%20Statement%20English.pdf.

[38] *Report of the 2014 Statutory Review of the Access to Information and Protection of Privacy Act Newfoundland and Labrador*, March 2015 pp. 309-313: http://www.ope.gov.nl.ca/publications/pdf/ATIPPA_Report_Vol2.pdf.

[39] *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, May 2016: https://www.leg.bc.ca/content/CommitteeDocuments/40th-parliament/5th-session/foi/Report/SCFIPPA_Report_2016-05-11.pdf : On March 8, 2017 the BC Government introduced an amendment to the *Information Management Act* S.B.C. 2015, c. 27 (Bill 6) that includes a small part of the proposed duty to document. It requires documentation of all decisions but fails to require documentation of actions and deliberations and does not provide for any oversight. A copy of Bill 6 is available at: https://www.leg.bc.ca/parliamentary-business/legislation-debates-proceedings/40th-parliament/6th-session/bills/progress-of-bills

C. vii Disregarding a Request

Problem

Periodically, requesters may make requests that are frivolous, vexatious, or otherwise abusive. Requests that are repetitious or systematic in nature can have significant consequences particularly for a small public body or municipality. Currently, the only remedy available under the law is a time extension in limited circumstances. Adding a permission to ignore frivolous and vexatious requests based on an authorization from the Commissioner provides a more effective means of managing these types of requests while ensuring that this extraordinary remedy is only granted through independent oversight.

Nova Scotia's *Personal Health Information Act* contains two provisions that permit health custodians to disregard frivolous and vexatious access requests and frivolous and vexatious correction requests. The Nova Scotia *PHIA* provisions are not consistent with the majority of other Canadian jurisdictions which require the permission of the Commissioner before a public body or health custodian is permitted to disregard a request.

Other Jurisdictions

Numerous jurisdictions across Canada have provisions allowing public bodies to seek permission to ignore requests that are an abuse of process. Abuse of process generally describes requests that are frivolous, vexatious, or sometimes repetitive. Despite some concern that the *FOIPOP* process is frequently abused by this type of requester, where public bodies can ask for permission to ignore this type of request, the requests are uncommon. Recent annual reports from three jurisdictions contain statistics summarized below that illustrate this point:

Jurisdiction	Legislation	# of requests for permission to ignore received in 1 year period
Alberta[40]	*Freedom of Information and Protection of Privacy Act*	3
	Health Information Act	1
	Personal Information Protection Act	2
British Columbia[41]	*Freedom of Information and Protection of Privacy Act* and *Personal Information Protection Act*	3
New Brunswick[42]	*Right to Information and Protection of Privacy Act*	4

[40] Alberta OIPC Annual Report pp. 26-27 for 2015-2016 available at: https://www.oipc.ab.ca/media/762451/Annual_Report_2015-16.pdf.
[41] OIPC British Columbia Annual Report 2015-2016 at p. 25 available at: https://www.oipc.bc.ca/media/16884/oipc_ar2015-16_6132_final_online.pdf.
[42] New Brunswick OIPC Annual Report 2014 at p. 20 available at: http://www.info-priv-nb.ca/userfiles/Annual%20Report%202013-2014.pdf.

While there are a variety of approaches taken to this issue in jurisdictions across Canada, there are two elements common to most of these provisions – they permit public bodies to disregard requests that:

- Would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the requests.
- Are frivolous or vexatious.

A number of jurisdictions also permit public bodies to disregard requests that are:

- Excessively broad or incomprehensible.
- Not made in good faith.
- Concern a trivial matter.
- Amount to an abuse of the right to access.

Recently, both Newfoundland and Saskatchewan have added new authorizations to disregarding access requests. In both cases the common elements include a requirement for authorization from the Commissioner and criteria including repetitious, frivolous, vexatious, or not in good faith.

Recommendation #10: Authorization to disregard requests
Add a provision to *FOIPOP* and the *MGA* that allows for public bodies and municipalities to disregard requests that would amount to an abuse of process with the permission of the Commissioner.

C. viii Open Data & Open Government

Problem
Access to information via a formal access to information request should be a last resort, a safety net to ensure that, if all else fails, there is a formal access process subject to independent oversight available to citizens. The access to information process is time consuming and costly for citizens and government. In addition, from an openness and accountability perspective, it is pro-active disclosure of information in the form of open data and open government initiatives that provides the most timely information about what government is doing on behalf of citizens. Nova Scotia's provincial government departments for example, have published extensive information on their websites. However, the information is scattered across the various websites and is often difficult to find. To try to make the information more accessible to citizens, the Office of the Information and Privacy Commissioner (OIPC) publishes a regularly updated list of interesting publicly available government information entitled, *Government Disclosures Available Online.*[43]

FOIPOP requires that public bodies publish directories to assist citizens in identifying and locating records.[44] Such directories can be an important and useful source of information for citizens. However, despite the fact that this provision is mandatory, these directories have not been created. It appears that the problem may be that *FOIPOP* also requires that only public bodies prescribed by regulations are required to publish these directories and no public bodies have ever been prescribed.

[43] Located on the OIPC website at: https://foipop.ns.ca/sites/default/files/Proactive%20Disclosure/16-00108%20Proactive%20release%20-%20Table%20-%20public%20disclosure%202016%20Sep%2008%20JY.pdf
[44] *FOIPOP* s. 48(1) and (2).

In Nova Scotia the Department of Internal Services produces an annual statistical report of government's processing of access to information requests. Included in that report is some information about government departments, agencies, boards, and commissions and some information about municipalities. There is no statutory requirement for this report and historically the report has been produced months, if not more than a year after the reporting period. Timely information regarding the performance of government is far more meaningful and serves the purposes of transparency.

Other Jurisdictions

Newfoundland's new access law has two provisions that are intended to promote more openness and accountability by public bodies: a publication scheme and a requirement for annual reporting by the Minister responsible for the Act. The Newfoundland publication provision differs from Nova Scotia in that it includes a requirement that the Commissioner create the standard template for the publication of information by public bodies. Further, the Commissioner is given oversight authority to ensure that the public bodies comply with the publication requirement.[45]

As noted earlier, recently a Special Committee of the British Columbia Legislative Assembly conducted an extensive review of the *Freedom of Information and Protection of Privacy Act*. In its final report, the Committee noted that open government can save time and money as well as improve trust in government if the processes for creating records in the first place are designed to support both accountability and access. The Committee stated that, "…all public bodies should view their information responsibilities in that light. Open and easy access to records and archives should be the norm. In principle, public bodies should be proactively disclosing records whenever disclosure is in the public interest."[46]

The BC Committee goes on to recommend a strengthening of the public interest override (discussed below in the Nova Scotia context) and an establishment of a publication scheme.

Recommendation #11: Open government

a) Amend *FOIPOP* to ensure that the Commissioner has oversight over public body compliance with the publication requirement set out in s. 48.
b) Add a provision to *FOIPOP* requiring that the Minister responsible for the Act deliver an annual statistical report regarding government's performance to the House of Assembly. Require that the report be published within four months of year end.
c) Remove s. 48(7) and provide, at a minimum, that all government departments must comply with the publication requirement without a need for any further regulation.

C. ix Mandatory Public Interest Override

Problem

Section 31 of *FOIPOP* and s. 486 of the *MGA* are the current public interest override provisions. Both are discretionary. The OIPC is unaware of any occasion when information has been disclosed in the past 23 years pursuant to either of these provisions. Modern access rules ensure that government has a positive obligation to disclose certain types of information in the public interest.

[45] *Access to Information and Protection of Privacy Act*, SNL 2015 C. A-1.2 s. 95(1)(b) and 95(3).
[46] *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, May 2016 at p. 16.

Another aspect of this problem is that when discretionary exemptions are found to apply to information, public bodies and municipalities generally fail to consider whether or not the public interest should prevail and the information should be disclosed despite the fact that the exemption is discretionary and public interest is a valid consideration in exercising discretion in favour of disclosure.

Other Jurisdictions

There are two types of public interest provisions in access laws in Canada. The first type is a general requirement to disclose information whether or not an access request has been made. Nova Scotia, British Columbia, Alberta and Ontario all have this type of provision.[47] However, Nova Scotia's version is the only version that is discretionary. The other three jurisdictions have a mandatory public interest override.

The second type of public interest override provides that even where an exemption may apply, the public body must consider the public interest before finally deciding whether or not to apply the exemption. Generally, these provisions list the exemptions that do not apply where a "compelling public interest" or "clearly demonstrated public interest" in disclosure outweighs the purpose of the exemption.[48]

The Newfoundland ATIPPA Review Committee determined that, "…in a modern law and one that reflects leading practice in Canada and internationally, it is necessary to broaden the public interest override and have it apply to most discretionary exemptions. This would require officials to balance the potential for harm associated with releasing information on an access request against the public interest in preserving fundamental democratic and political values. These include values such as good governance, including transparency and accountability; the health of the democratic process; the upholding of justice; ensuring the honesty of public officials; general good decision making by public officials. Restricting the public interest to the current narrow list implies that these other matters are less important."[49]

Recommendation #12: Public interest override

a) Make the public interest override provision mandatory.
b) Add a new provision requiring public bodies and municipalities to always consider the public interest before exempting information under a discretionary exemption.

[47] See Appendix 1 for the text of these provisions.
[48] Laws in Newfoundland and Ontario contain these types of provisions listed in Appendix 1.
[49] *Report of the 2014 Statutory Review of the Access to Information and Protection of Privacy Act Newfoundland and Labrador*, March 2015, p. 78.

D. Modernizing Privacy Rights

i. Standards for Sharing Personal Information
ii. Modern Protections for Personal Information
   a) Core Privacy Standards
   b) Mandatory Privacy Impact Assessments
   c) Information Sharing Agreements
   d) Privacy Management Program
   e) Mandatory Breach Notification
   f) Mandatory Consultation on Draft Legislation
   g) Direct Collection and Notification
   h) Personal Information Banks

D. i Standards for Sharing Personal Information

Problem

There are three problems with Nova Scotia's public sector access laws in relation to the sharing of personal information: weak standards for sharing between public bodies, no appropriate standards to permit the delivery of common or integrated services or activities, and no standards to permit the use of big data while protecting privacy.

First, the standard for sharing of personal information between Nova Scotia's public bodies is vague and fails to adequately protect the privacy of citizens. Section 27(f) of *FOIPOP* and s. 485(2)(f) of the *MGA* permits sharing between public bodies or between municipalities if the information is necessary for the performance of the duties of or for the protection of the health or safety of the officer or employee of the public body or municipality. Information may also be shared between public bodies to meet the necessary requirements of government operations. These standards are well below the requirements of other modern privacy laws in Canada.

Second, the information sharing provisions in *FOIPOP* are not well suited to modern citizen-centric service delivery programs. Nova Scotia's public bodies seek to improve delivery of citizen-centered services. In doing so, they seek to combine or share personal information using technology. This type of sharing for common or integrated programs or activities could be facilitated by a specific statutory authorization and specific privacy protection and oversight. Further, Nova Scotia is working towards developing an online identity service that would be used by multiple public bodies – a shared service for the benefit of citizens.

Third, government departments, municipalities and other large public bodies are acquiring more and more data. With data comes a desire to manipulate it, combine it, mine it and use it. Nova Scotia's 20 year old privacy laws were not designed with big data practices in mind. As it currently stands, many of the information practices involved in big data would not be compliant with the privacy protections set out in Nova Scotia's public sector privacy laws. The current legislative framework is based on a set of protections that in effect require public bodies to act as "silos" of personal information. These protections include the requirement that collection of personal information must be "necessary", secondary uses are restricted, information sharing is limited, and information must be accurate, complete and up to date.[50] While it may be possible to still engage in some big data projects, in general such projects would only be possible if authorized under another

[50] *Big Data Guidelines May 2017,* Office of the Information and Privacy Commissioner of Ontario at p. 3.

law. To allow for big data type practices in general, a new or modified legislative framework is needed.

Any new privacy provisions that facilitate big data projects must take into account the privacy risks of big data such as the use of poorly selected data sets that lack information or are incomplete, contain incorrect or outdated information or disproportionately represent certain populations. Unless these projects are properly designed they may incorporate implicit or explicit biases or generate pseudo-scientific insights that assume correlation equals causation. In addition, they often lack transparency regarding the inner logic of the system. If not designed properly, big data projects can result in uses of personal information that may be unexpected, invasive and discriminatory.[51]

Because of the lack of key modern privacy protections in Nova Scotia, sharing of personal information through these types of programs is occurring and it is happening with no oversight by or consultation with the Commissioner.

Other Jurisdictions

The standard for sharing between public bodies and municipalities in Nova Scotia is the standard reserved only for sharing within a public body or municipality in other jurisdictions including Newfoundland, British Columbia and Ontario.[52]

Other jurisdictions have provisions that specifically permit sharing of personal information for the purposes of delivering common or integrated programs or activities. Newfoundland and New Brunswick both permit disclosures for these purposes.[53] The British Columbia law provides a better approach because it requires key privacy protections including the requirement for a mandatory privacy impact assessment and a requirement that these PIAs be provided to the Commissioner for comment. The law also requires that public bodies provide the Commissioner with early notification of plans to develop a common or integrated program or activity. Each of these elements serve to facilitate the development of these programs while ensuring that the privacy of citizens is considered and protected.[54]

British Columbia's public sector access law allows for collection for prescribed purposes, for the purpose of planning for or evaluating a program and where the information is personal identity information collected by a provincial identity information service provider. The Act authorizes the Minister to designate a public body as the provincial identity information service provider and it sets out the permitted activities of such an entity. As a result, the provisions put statutory limits on the collection while facilitating the use of a provincial identity information service provider.[55]

---

[51] All of these concerns were raised by the Information and Privacy Commissioner for Ontario in his recent presentation for Data Privacy Day available at https://www.ipc.on.ca/wp-content/uploads/2017/01/2017-01-26-privacy-day-commissioner-presentation-final.pdf.

[52] British Columbia's *Freedom of Information and Protection of Privacy Act* s. 33.1(1)(e) and (e.1), Newfoundland's *Access to Information and Protection of Privacy Act* s. 68(1)(f), Ontario's *Freedom of Information and Protection of Privacy Act* s. 42(1)(d) all available in Appendix 1.

[53] Newfoundland's *Access to Information and Protection of Privacy Act* s. 68(1)(u) and New Brunswick's *Access to Information and Protection of Privacy Act* s. 46(1) available in Appendix 1.

[54] See s. 33.1(d), Schedule 1 (definition of "common or integrated program or activity") and s. 69(5.2), (5.4), (5.5) of British Columbia's *Freedom of Information and Protection of Privacy Act* available in Appendix 1.

[55] See s. 26(d), (e) and (h), and s. 69.2 of British Columbia's *Freedom of Information and Protection of Privacy Act* available in Appendix 1.

Recently, the Information and Privacy Commissioner for Ontario discussed the advantages of big data, while highlighting the limitations of outdated privacy laws and the privacy risks inherent in the use of big data. He recommends the creation of a principled-based legislation governing data-linking and big data analytics which could include five core safeguards:

- Creation of a data institute or institutes with expertise in privacy, human rights, and ethical issues involved in data integration and analytics.
- Requirement for data minimization.
- Mandatory privacy impact assessments and threat risk assessments.
- Mandatory breach notification and reporting to the IPC and the affected individuals.
- Order making and audit powers for the Information and Privacy Commissioner.[56]

Recommendation #13: Standards of sharing personal information

a) Repeal ss. 27(f) and 27(g) of *FOIPOP* and ss. 485(2)(f) and 485(2)(g) of the *MGA* and replace those provisions with provisions that permit disclosure within the public body or within the municipality where the information is necessary for the performance of the duties of the employee of or service provider to the public body or municipality.

b) Add new provisions that permit disclosure for the purposes of the delivery of a common or integrated program or service. Add a definition of common or integrated program or activity that requires documentation of the program and a privacy impact assessment. Require public bodies to notify the Commissioner as early as possible of any proposed common or integrated program or activity. Make privacy impact assessments mandatory for any common or integrated program or activity and require public bodies to provide a copy of the privacy impact assessment for comment by the Commissioner.

c) Add a new provision that permits disclosure of personal information to a provincial identity service provider. Authorize the Minister responsible for the Act to designate a public body as the provincial identity service provider and set out the permitted activities of such an entity. The amendments should include limitations on the collection of personal information by the provincial identity service provider.

d) Add a new provision that permits disclosure of personal information to a big data institute. Define the nature of the institute and require that it include privacy, human rights, and ethical expertise in data integration and analytics. Include a requirement for data minimization, mandatory privacy impact assessments to be provided to the Commissioner, and threat risk assessments for all big data initiatives. Include these initiatives in the mandatory breach notification process.

D. ii Modern Protections for Personal Information

Problem

The threats to personal information in 2017 are vastly different than those that existed 1993. Likewise, the potential for harm has risen exponentially with the scope of data now collected by public bodies. One portable storage device can contain the personal information of hundreds of thousands of citizens. The loss or theft of such a device can be extremely costly to the individuals affected and to the public body. Privacy laws across Canada have addressed this issue by adding a number of key privacy protections to their updated laws:

a. Core privacy standards
b. Mandatory privacy impact assessments
c. Mandatory information sharing agreements

[56] Government and Big Data: Privacy Risks and Solutions, https://www.ipc.on.ca/wp-content/uploads/2017/01/2017-01-26-privacy-day-commissioner-presentation-final.pdf .

d. Privacy management program requirements
e. Mandatory breach notification
f. Mandatory consultation on draft legislation
g. Direct collection and notifications
h. Personal information banks

Nova Scotia's access laws contain none of these essential modern privacy protections.

D. ii a Core Privacy Standards

Problem
Essential to any modern privacy law are three core privacy standards once considered best practice, but now considered, in many jurisdictions, mandatory standards:

- Don't collect, use, or disclose personal information if other information will serve the purpose.
- Collect, use, and disclose the minimum personal information necessary.
- Disclose information within your organization on a need to know basis only.

Nova Scotia has already recognized these core standards in the *Personal Health Information Act.*[57]

Recommendation #14: Core privacy standards
Add three core privacy standards to *FOIPOP* and the *MGA*:
a) Prohibit collection, use, or disclosure of personal information if other information will serve the purpose.
b) Limit collection, use, and disclosure of personal information to the minimum personal information necessary.
c) Permit disclosure of personal information within an organization only on a need to know basis.

D. ii b Mandatory Privacy Impact Assessments

Problem
There is no mandatory requirement in our privacy laws requiring public bodies and municipalities to conduct an assessment of the privacy implications of new projects, programs, systems, or legislation prior to undertaking these new initiatives. This means that, for example, 70% of municipalities in Nova Scotia engage in video surveillance and none of them evaluated the privacy implications of this highly privacy invasive technology before implementing the technology.[58] No assessment was done of the purpose, scope, retention period, access to or security of the video surveillance. As the scope and sensitivity of personal information collection grows, so too does the need to ensure that any collection, use, or disclosure of personal information is authorized under our laws, that privacy risks are identified and that appropriate mitigation plans are implemented. Privacy impact assessments are internationally recognized tools that permit such an assessment to occur. These assessments also help identify privacy risks early and require the development of a mitigation strategy before it is too late.

[57] *Personal Health Information Act* ss. 24 and 25 reproduced below in Appendix 1.
[58] The OIPC conducted an informal survey of the use of video surveillance by all municipalities in 2016. Twenty-five of the 53 municipalities responded to the survey and 17of the 25 reported using video surveillance.

Other Jurisdictions
Newfoundland and British Columbia are two examples of jurisdictions that require public bodies to complete privacy impact assessments for new projects, programs, and systems and further, that specifically require privacy impact assessments for all common or integrated programs or activities.[59]

In the recently approved *General Data Protection Regulation* (*GDPR*), the European Parliament set out its rules for the processing of personal data. One of the protections included in the *GDPR* is the requirement for a data protection impact assessment particularly where the processing of data is likely to result in a high risk to the rights and freedoms of natural persons.[60]

Recommendation #15: Privacy impact assessments
a) Require that public bodies and municipalities complete a privacy impact assessment on all new projects, programs, systems, enactments, and activities.
b) Require that public bodies that are government departments submit their privacy impact assessments to the Minister responsible for the Act for the Minister's review and comment.
c) Where the proposed program, project, system, or activity involves a common or integrated program or activity, require that the privacy impact assessment be provided to the Commissioner for comment (consistent with recommendation #12(b) above).
d) Where the proposed program, project, system, or activity involves big data, require that a privacy impact assessment be completed and provided to the Commissioner for comment (consistent with recommendation 13(d) above).

D. ii c Information Sharing Agreements

Problem
FOIPOP and the *MGA* permit disclosure of personal information for the purpose of complying with an agreement made pursuant to an enactment. Information sharing agreements are standard privacy management documents used to clearly identify the authorities for regular sharing of personal information between public bodies or with other organizations and to set out the terms and conditions for such sharing. They provide essential protection to citizens and a degree of transparency when these documents are subject to independent oversight. Neither *FOIPOP* nor the *MGA* prescribe any requirements with regard to the completion of these types of agreements.

Modern privacy legislation sets out core elements required in any information sharing agreement including a definition of the specific data elements of personal information being shared, the specific purposes for the sharing, clear limitations on the secondary use and onward transfer, and an outline of other measures often prescribed in regulations including specific safeguards, retention periods, and other accountability measures. Nova Scotia's privacy laws contain none of these requirements.

Other Jurisdictions
Ontario's public sector law focusses the agreement requirement on service provider organizations. It prohibits a person who provides services on behalf of a service provider organization from

[59] Common and integrated programs or activities and the need for a privacy impact assessment requirement is discussed above in section D.i. – Standards for Sharing Personal Information. Examples of the general provisions requiring completion and review of privacy impact assessments can be found in Appendix 1.
[60] Official Journal of the European Union, Article 35, Regulation (EU) 2016/679 of the European Parliament and of the Council (27 April 2016).

collecting personal information in connection with providing services unless the person and the service provider organization have entered into an agreement in compliance with prescribed requirements.

British Columbia mandates the use of information sharing agreements in accordance with the directions of the Minister responsible for the Act. The Minister has created a mandatory template agreement.[61]

Recommendation #16: Information sharing agreements

a) Amend *FOIPOP* and the *MGA* to require that any regular sharing of personal information by public bodies or municipalities be in writing in the form of information sharing agreements. Include requirements regarding the content of the information sharing agreements.
b) Require public bodies and municipalities to notify the Commissioner of all new or amended agreements to share personal information and give the Commissioner explicit authority to review and comment on the agreements.
c) Require publication of the existence and nature of the information sharing agreements between public bodies, municipalities, and with other external bodies.

D. ii d Privacy Management Program

Problem

Nova Scotia's public sector privacy laws were drafted long before the idea that a privacy management program is the most effective way to ensure compliance with privacy rules. Nova Scotia's *PHIA* mandates implementation of some elements of privacy management programs such as the requirement to implement, maintain, and comply with information practices that meet the requirements of the Act, are reasonable in the circumstances, and ensure that personal information is reasonably safeguarded. Custodians under *PHIA* must have a complaints policy, retain a record of user activity, and provide public information about their privacy practices including contact information of the privacy lead for the organization.[62] These are exactly the type of privacy management protections that can and should be added to public sector privacy laws. *FOIPOP* and the *MGA* do not have these requirements.

Other Jurisdictions

The Yukon Information and Privacy Commissioner also recently prepared recommendations for the modernization of the Yukon's public sector access and privacy law. Included in her recommendations was the following:

> Recommendation #3
> The ATIPP Act should require Yukon Public Bodies to develop and maintain a privacy management program consisting of:
> - the ability to demonstrate accountability for privacy management through executive management support, designation of a privacy officer, and development of a reporting structure in respect of the privacy officer's activities;

[61] Directions for the completion of information sharing agreements from the Minister responsible for the Act are available at: http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-overnment/information-management-technology/information-privacy/resources/policies-guidelines/information-sharing-agreements-guidelines.pdf.
[62] *Personal Health Information Act*, SNS c. 41 2010 ss. 61-68.

- a personal information inventory and program controls: privacy policies and procedures, use of risk management tools (PIAs, security threat risk assessments, and ISAs); employee training programs and tools, service provider management, and external communications to the public including: privacy policies and procedures; notices about collection, use and disclosure of personal information, and information about rights and how to exercise them; and
- an oversight and review plan to identify and address deficiencies in the program.[63]

Currently there is no statutory requirement under British Columbia's privacy law for public bodies to implement the essential elements of a privacy management program. But the former Information and Privacy Commissioner for British Columbia, Elizabeth Denham, in her submissions to the Special Committee tasked with reviewing BC's *FIPPA* noted:

> Citizens often have little to no choice about providing their personal information to public bodies, regardless of whether that entity has a poor or good record of protecting the privacy of citizens.
>
> A privacy management program is, for a person's private information, very similar to a financial management program, dealing with public finances.
>
> The case for the inclusion of a privacy management program in FIPPA is arguably even stronger than it is under PIPA. In the privacy sector, citizens can be selective about who they trust with their personal information, they can seek one of many private sector providers. In contrast, in most instances, there is no choice in the public sector.[64]

The BC Commissioner's recommendations were accepted by the Special Committee who in turn recommended adoption of these requirements.[65]

Recommendation #17: Privacy management program requirements
Add a requirement that public bodies and municipalities have a privacy management program that:
a) Designates one or more individuals to be responsible for ensuring that the public body or municipality complies with *FOIPOP* and the *MGA* from within the organization.
b) Is tailored to the structure, scale, volume, and sensitivity of the personal information collected by the public body or municipality.
c) Includes policies and practices that are developed and followed so that the public body or municipality can meet its obligations under *FOIPOP* or the *MGA*, and makes policies publicly available.
d) Includes mandatory privacy training for all employees.
e) Has a process to respond to complaints that may arise respecting the application of *FOIPOP* or the *MGA*.
f) Is regularly monitored and updated.

---

[63] Yukon Information and Privacy Commissioner, *Access to Information and Protection of Privacy Act 2015 Review: Information and Privacy Commissioner's Comments*, at p. 28. Available at: http://www.ombudsman.yk.ca/uploads/media/561eea31db69c/Comments_Web%20Version.pdf?v1.
[64] Elizabeth Denham, Information and Privacy Commissioner for British Columbia, *Statutory Review of the Freedom of Information and Protection of Privacy Act, Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act,* November 18, 2015 available at: https://www.oipc.bc.ca/special-reports/1884.
[65] Legislative Assembly of British Columbia, *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, May 2016 Recommendation 22, p. 62.

D. ii e Mandatory Breach Notification

Problem

There is currently no mandatory breach notification requirement under *FOIPOP* or the *MGA*. Neither individuals affected by breaches nor the Commissioner receive regular notification of breaches. In 2016/17 the Office of the Information and Privacy Commissioner received only three breach reports from public bodies in Nova Scotia. The OIPC has never had an individual complain to this office because he or she received a breach notification letter directly from a government department. It is simply impossible that privacy breaches are not happening in Nova Scotia. Based on a scan of the publicly reported breaches in other Canadian jurisdictions, I estimated that Nova Scotia government departments suffered as many as 154 breaches in 2015, of which 10 were significant.[66] As other jurisdictions modernize their privacy laws, they have included mandatory breach notification as part of the improvements. Indeed, when Nova Scotia passed the *Personal Health Information Act* in 2010, it recognized the need for breach notification, even if the notification provisions require revision.[67]

Other Jurisdictions

Key elements of current Canadian standards of notification to Commissioners require:

- Prompt notification (first reasonable opportunity, as soon as feasible, without unreasonable delay) of Commissioner of material breaches or breaches involving a "real risk of significant harm."
- Detailed notification content, including notice of right to complain to the Commissioner.
- Organizations must retain a record of all data breaches that the Commissioner can inspect.[68]
- Notify third parties who the organization believes might be in a position to mitigate the risk of harm.

In Appendix 1 I have summarized the breach notification provisions in five Canadian access laws. My recommendation below takes into account the best of these practices.

Recommendation #18: Mandatory privacy breach notification

a) Require notification to affected individuals and the Commissioner, without unreasonable delay, of all privacy breaches involving a real risk of significant harm.
b) Specify content requirements for notification to individuals including: details about the cause of the breach, a list of the type of data lost or stolen, an explanation of the risks of harm affected individuals may experience as a result of the breach, and information about the right to complain to the Commissioner.
c) Authorize the Commissioner to order notification to an individual affected by the breach.
d) Require maintenance of a record of all data breaches with specified details available to the Commissioner upon request.

---

[66] Discussed in more detail in 2015-2016 Annual Report of the Office of the Information and Privacy Commissioner at pp. 7-8 available at: https://foipop.ns.ca/sites/default/files/publications/annual-reports/OIPC%202015-2016%20Annual%20Report.pdf.

[67] *Personal Health Information Act*, SNS 2010, c. 41 ss. 69-70.

[68] *Digital Privacy Act*, SC 2015, c. 32, s. 10.3(1), European Union, General Data Protection Regulation Article 33(5)).

D. ii f Mandatory Consultation on Draft Legislation

Problem

Currently the Nova Scotia Government does not consult the OIPC in advance of introducing legislation that may have significant privacy or access implications. For example, when the *Privacy Review Officer Act* was passed granting the Commissioner oversight over the privacy provisions in *FOIPOP*, the OIPC was not consulted and did not know about the new powers until a regular scan of new legislation by the office uncovered the new law after it was passed. Another typical example is that legislation frequently and unnecessarily notwithstands *FOIPOP*. Such provisions must be carefully scrutinized or the privacy and access rights of citizens will become less and less meaningful. As former Alberta Information and Privacy Commissioner Frank Work said,

> Left unchecked, the practice of taking other enactments out of FOIP by making them "paramount" to FOIP has the potential to turn FOIP into "a piece of Swiss cheese", causing its death "by a thousand cuts" or bringing about its virtual "repeal by degrees."[69]

Other Jurisdictions

A number of Canadian privacy laws now include an explicit requirement for government to consult its Privacy Commissioner as it prepares new legislation or the legislation provides a specific authority for the Commissioner to comment on legislative schemes. The most recent of these new provisions is found in Newfoundland's law. The Privacy Commissioner of Canada has recommended that the *Privacy Act* be amended to include this requirement.[70]

Recommendation #19: Mandatory consultation on draft legislation

a) Impose a duty on Ministers to consult with the Commissioner on any proposed Bill that could have implications for access to information or protection of privacy prior to introduction into the House.
b) Provide the Commissioner with the necessary general power to comment on the implications for access to information or for protection of privacy of proposed legislative schemes.

D. ii g Direct Collection and Notifications

Problem

Our current laws do not require public bodies and municipalities to collect personal information directly from individuals. Nor do our laws require that individuals be given notice when personal information is being collected directly from them. Finally our laws fail to specify when indirect collection is permitted. These are all important limitations on the power of the state to collect personal information. At their essence, these collection rules recognize the inherent dignity of individuals by providing them with information at the time of collection about the purpose of and authority for the collection.

---

[69] Contained in the introduction to a 2011 study on Paramountcy clauses conducted by the Office of the Information and Privacy Commissioner for Alberta and quoted in that Office's 2013 submission to Government of Alberta *FOIPOP* Review at p. 16. https://www.oipc.ab.ca/media/387450/review-of-the-foip-act-becoming-a-leader.pdf.

[70] *Privacy Act Reform in an Era of Change and Transparency*, Office of the Privacy Commissioner of Canada at p. 9: https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_sub_160322/.

Other Jurisdictions
Virtually every other jurisdiction in Canada requires that personal information be collected directly from the individual unless the law authorizes another method of collection. Indeed, even one of Nova Scotia's privacy laws, *PHIA*, requires it.[71]

Two typical examples are Ontario and Newfoundland. Both laws require direct collection, specify the limited circumstances in which indirect collection is authorized, and set out information that must be communicated via direct notice to individuals.[72]

Recommendation #20: Collection notification
a) Add a requirement to *FOIPOP* and the *MGA* that personal information must be collected directly from the individual the information is about unless the law authorizes another method of collection.
b) Where information is collected directly from an individual, require that the public body or municipality tell the individual from whom it collects personal information the purpose for collecting it, the legal authority for collecting it, and the contact information of an individual who can answer any questions.

D. ii h Personal Information Banks

Problem
Part of the mandate of the Information and Privacy Commissioner for Nova Scotia is to undertake research in matters concerning privacy legislation and inform the public about the Act.[73] As a result, in the past two years we have met with almost 2000 individuals in Nova Scotia who play some role in the administration of access and privacy laws. During our discussions with these public servants it has become clear that public bodies have not been in the practice of conducting audits of their personal information collection. As a result, many are not aware of the nature, amount, and location of the personal information collections held by their organizations. It is not possible to properly protect personal information if you don't know where it is or what it is. So while this recommendation is focused on ensuring that the public is made aware of the scope of the collection, implementation of this recommendation will have the collateral benefit of ensuring that all public bodies and municipalities have a complete audit of their personal information collections.

As public bodies and municipalities collect and combine more and more personal information, it is essential that that information is properly protected as required under the privacy rules in *FOIPOP* and the *MGA*. The first step in doing so is to have a complete list of all personal information banks. Such lists should be made publicly available so that citizens are aware of the extent and scope of personal information collections by government. Further, best practice requires that such lists include authority for collection and a list of all intended uses and disclosures with an explanation of the authority for each.

Interestingly, Nova Scotia's *FOIPOP* already includes a requirement for the creation of personal information banks that includes a list of essential data elements. It has not ever been used it appears because s. 48(7) of *FOIPOP* also currently requires that public bodies required to produce

[71] *Personal Health Information Act*, SNS 2010, c. 41 s. 31.
[72] Section 39 of Ontario's *Freedom of Information and Protection of Privacy Act* and s. 62 of Newfoundland's *Access to Information and Protection of Privacy Act* are set out in Appendix 1. Other examples include PEI (s. 32), New Brunswick (s. 38), Manitoba (s. 37(1)), and Alberta (s. 34(1), Saskatchewan (s. 26(1)).
[73] *Privacy Review Officer Act*, SNS 2008, c. 42, s. 5(1)(d) and (e).

personal information banks must be prescribed by regulation and no regulation has ever been put into effect.

Recommendation #21: Personal information banks

a) Repeal s. 48(7) so that the requirement for personal information banks applies to all public bodies and without any further legislative effort (consistent with recommendation 11(c)).
b) Require that municipalities publish and maintain personal information banks.

E. Improving Oversight

i. Independence of Oversight Agency
   a) Officer of the Legislature
   b) Name Change
   c) Employees, Experts, and Support
   d) Restrictions on Disclosure and Immunity
ii. Order Making versus Recommendation Making Power
iii. Powers on Conducting Investigations or Reviews
   a) Power to Determine Own Procedure
   b) Power to Compel Production of Records
   c) Information Sharing with Other Commissioners
   d) Grounds to Refuse to Conduct or Continue a Review
   e) Time Limits on Commissioner's Processes
iv. General Powers of the Commissioner

E. i Independence of Oversight Agency

There are four areas where Nova Scotia's law could be improved to ensure the independence of the Office of the Information and Privacy Commissioner for Nova Scotia in a manner consistent with other Canadian jurisdictions.

E. i a Officer of the Legislature

Problem
One of the core purposes of *FOIPOP* and the *MGA* is to provide for an independent review of decisions made pursuant these Acts.[74] Independence requires security of tenure and financial independence from those subject to oversight. In Nova Scotia, the Commissioner files her annual report with the House of Assembly, but is required to seek budget approvals through the Department of Justice – a Department over which she has oversight. This significantly undermines the perception and reality of the independence of the office.

Other Jurisdictions
All jurisdictions in Canada except Nova Scotia have made the Information and Privacy Commissioner an officer of their legislature.

Recommendation #22: Officer of the legislature
Make the Information and Privacy Commissioner (Review Officer and Privacy Review Officer) an officer of the legislature.

E. i b Name Change

Problem
FOIPOP, the *MGA*, *PRO*, and *PHIA* all refer to a Review Officer or a Privacy Review Officer. That title is often used within government for individuals tasked with internal review responsibilities. As a result, there is significant confusion within government and with the public as to who exactly the "Review Officer" is. Ministers, deputy ministers, media, and citizens all confuse the role of the

[74] *FOIPOP* s. 2(a)(v), *MGA* s. 462(a)(v).

Review Officer and often believe the job is responsible for processing access requests. As recently as October 2016, the assembly debates reveal that members of the legislature continue to confuse the independent oversight agency with those who process access requests on behalf of the government.[75]

Other Jurisdictions
No other jurisdiction in Canada uses the title "Review Officer" for this oversight role. All common law provinces and the federal government use the term Information and Privacy Commissioner or Ombudsman to describe the person responsible for independent oversight of access and privacy rules. As a result, beginning in the fall of 2015, the FOIPOP Review Office changed its name to the Office of the Information and Privacy Commissioner. The change was communicated on our website, through social media and in all of our letters and communications sent out in the six months following the change. While this informal name change has resulted in some improvement in the understanding of our role, a formal change in law is necessary.

Recommendation #23: Name change
Change the name of the oversight body in *FOIPOP* with necessary consequential amendments to *PRO*, the *Personal Health Information Act* (*PHIA*) and the *MGA* to "Information and Privacy Commissioner".

E. i c Employees, Experts, and Support

Problem
Independent officers require exactly that, independence from government to ensure that their decisions are free of any undue influence. This is particularly true in two key areas: hiring and classification of employees, and hiring and payment for experts.

In Nova Scotia the need for independence in relation to these issues is enshrined in provisions found in the *Auditor General Act* and the *Elections Act*.[76]

One further provision missing from *FOIPOP* is the power of the Commissioner to delegate her responsibilities. A clear statement of that authority in *FOIPOP* would assist staff of the office as they undertake their delegated tasks which include investigation, mediation, and decision-making in relation to time extension matters as well as decisions regarding the scope of our jurisdiction. Further, in small jurisdictions such as Nova Scotia, there is a real possibility that, from time to time, the Commissioner herself may be in a conflict of interest. The power to delegate in these circumstances would allow the regular processes to continue through delegation.

Other Jurisdictions
There is no single approach to the authority given to Information and Privacy Commissioners across Canada in relation to the hiring and remuneration of staff and experts. However, it is not

[75] Assembly debates, Tuesday, October 18, 2016 at p. 136. In response to a question about expanding the powers and mandate of the FOIPOP Review Officer the Premier stated, "I want to thank all those FOIPOP officers across the government who continue to ensure that the data and information that is being asked for…is being provided to them as quickly as possible." The FOIPOP Review Officer is the Information and Privacy Commissioner. There is only one Information and Privacy Commissioner and she does not process access requests for government.
[76] Copies of the relevant provisions can be found in Appendix 1.

uncommon for there to be an express indication of authority to determine classification and remuneration and to hire experts.[77]

Other jurisdictions' laws include provisions that specifically authorize the Commissioner to delegate her authority. Examples include New Brunswick and Newfoundland, although numerous jurisdictions have similar provisions.[78]

Recommendation #24: Employees, experts, and support

a) Authorize the Commissioner to appoint employees she considers necessary in such positions she considers appropriate under such classification ratings and at such rates of remuneration within those classification ratings established by the Public Service Commissioner.
b) Authorize the Commissioner to engage the services of such counsel or other professionals or experts to advise or assist the Commissioner notwithstanding any government procurement rules or policies.
c) Authorize the Commissioner to delegate any of her powers except the power to delegate. Make clear that such delegation may occur when the Commissioner declares a conflict of interest.

E. i d Restrictions on Disclosure and Immunity

Problem

All modern access and privacy laws include a restriction on disclosure of information by the Commissioner and her staff as well as an immunity clause. While *FOIPOP* currently has an immunity clause, that clause only applies to "the head of a public body or any person acting on behalf of or under the direction of the head of the public body."[79] There is no statutory restriction on the disclosure of information gathered by the Commissioner in the course of her duties. There is a provision directing the Supreme Court when hearing an appeal to "take every reasonable precaution, including, where appropriate, receiving representations *ex parte* and conducting hearings *in camera*, to avoid disclosure by the Supreme Court" of any information or material of a record at issue or even of the fact of the existence of a record where the public body has not disclosed its existence.[80]

The Commissioner's office has maintained a practice of keeping records in strictest confidence because to do otherwise would undermine the core work of the office. Enshrining this practice in legislation would confirm for public bodies and citizens that information supplied to the Commissioner is received in confidence and will only be used in accordance with the restrictions specified under the law. Further, given the sensitivity of data and the increase in litigation regarding privacy, an immunity provision is necessary and in keeping with standards across Canada.

Other Jurisdictions

Examples of both types of provisions can be found in legislation across Canada. Examples from Newfoundland, British Columbia, Alberta, and Saskatchewan can be found in Appendix 1.

[77] Examples from Newfoundland, British Columbia, Ontario, New Brunswick, Saskatchewan, and PEI can be found in Appendix 1.
[78] See Appendix 1 for a copy of the relevant delegation provisions.
[79] *FOIPOP* s. 46(1).
[80] *FOIPOP* s. 42(3).

Recommendation #25: Restrictions on disclosure and immunity
Add a provision enumerating the permitted uses and disclosures of information by the Commissioner and her staff and a provision specifying the immunity of the Commissioner and her staff.

E. ii Order Making versus Recommendation Making Power

Problem
Having recommendation making power means that if public bodies or municipal bodies choose, they can simply ignore the Commissioner's recommendations. This has four significant consequences:

- The current standard creates a situation where the administrator whose decision is being reviewed is almost always the same person who decides whether or not the Commissioner's recommendations should be followed. In effect, this makes the decision maker the final arbiter of the correctness of the decision. This completely undermines the purpose of independent review. The Nova Scotia Supreme Court referred to this problem as an "anomalous situation".[81]
- Public bodies and municipalities are not required to provide reasons when they refuse to follow recommendations. On occasion, they have provided reasons that are irrelevant under the access rules. Most responses come with no explanation at all when the recommendation is rejected.
- Public bodies and municipalities are sometimes unwilling to engage in informal resolution because they know if they stick to their position and are subject to formal review by the Commissioner, they are not bound by the Commissioner's recommendation. Their failure to engage in informal resolution creates delays and may increase costs to the applicant and the public since it requires that the appeals go to formal review. In 2016, the OIPC's informal resolution rate was 87%. However, some public bodies had informal resolution rates as low as 50% because they failed to engage in meaningful informal resolution.
- Applicants bear the burden of appealing to the Supreme Court of Nova Scotia if public bodies refuse to follow the Commissioner's recommendation. This is an additional cost citizens must bear in the current process.

Other Jurisdictions
Eight jurisdictions in Canada use the ombudsman model. Five jurisdictions (Alberta, BC, Ontario, PEI, and Quebec) have order making power. In 2005, former Supreme Court of Canada Justice La Forest provided a report to the federal government regarding the two oversight models found in privacy laws and he stated,

> There is a danger that a quasi-judicial order making-model could become too formalized, resulting in a process that is nearly as expensive and time-consuming as court proceedings. It is also arguable that the absence of an order-making power allows the conventional ombudsman to adopt a stronger posture in relation to government than a quasi-judicial decision-maker. There is also some virtue in having contentious access and privacy issues settled by the courts, where proceedings are generally open to the public. The ability of both the commissioners and complainants to resort to the courts may well be seen to be a

[81] *Keating v. NS (AG)*, 2001 NSSC 85 at para 30.

sufficient sanction for non-compliance, particularly in relation to some of the more sensitive issues arising at the federal level.[82]

In Nova Scotia, the ombudsman model means that applicants, public bodies, and municipalities do not require legal counsel to present submissions to the Commissioner at the final stage of the process. The process is fair but informal. Material supplied during the informal resolution process is used by the Commissioner if the matter goes to formal review. This saves the parties from repeating their arguments. The disadvantage, as noted above, is that without order making power, some public bodies and municipalities fail to actively engage in informal resolution and others fail to comply with recommendations for reasons entirely unrelated to the access and privacy rules.

However, order making power would mean that the Commissioner would require significantly more resources to create an adjudication division completely separate from the informal resolution division of the office. This would be a significant expense for a jurisdiction that requires generally fewer than 20 formal reviews per year.

In recent reviews by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI Committee), the Information Commissioner of Canada and the Privacy Commissioner of Canada both recommended that their laws be updated to change their oversight model from an ombudsman model to an order making model.

Newfoundland recently adopted a new model that falls between an order making and a strictly ombudsman model. Newfoundland's new law maintains the recommendation making power of the Commissioner but requires that if a public body decides not to comply with a recommendation of the Commissioner, the public body must, within 10 business days after receipt of the recommendation, apply to the Trial Division for a declaration that it is not required to comply with the recommendation.[83] The obvious advantage of this approach is that it shifts the burden of going to court onto the public body. It adds gravitas to the Commissioner's recommendations because public bodies can now only refuse to follow the recommendations if they have reasons in law to support such a position. Finally, the Newfoundland approach ensures that, in a small jurisdiction, the informal resolution process can continue and the oversight body does not require additional funds to create an adjudication unit.

Recommendation #26: Authority of the Commissioner
Amend *FOIPOP* and the *MGA* to shift the burden onto the public body or municipality to seek a declaration of the Nova Scotia Supreme Court whenever the public body or municipality decides that it will not follow the recommendations of the Commissioner.

E. iii Powers on Conducting Investigations or Reviews

The powers originally granted to the "Review Officer" under Nova Scotia's access and privacy laws are dated and fail to include some powers found in more modern access and privacy laws. These powers would serve to ensure efficient, fair, and timely decision making by the Commissioner.

[82] Gerard V. La Forest, *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues* http://www.justice.gc.ca/eng/rp-pr/csj-sjc/atip-aiprp/ip/index.html.
[83] See Appendix 1 for a copy of the relevant provision.

E. iii a Power to Determine Own Procedure

Problem
FOIPOP and the *MGA* are silent on the issue of the Commissioner establishing her own procedures for reviews or complaint investigations. The OIPC has published a procedure document describing its processes.[84] In fairness to the parties it is important to make clear the power of the Commissioner to control procedures. Further, we are regularly challenged by public bodies, municipalities, and applicants regarding our authority to control our process. In order to efficiently manage ever growing caseloads with limited resources we need to ensure that we can focus the parties on specific issues and find meaningful fair resolutions. Control of our process and procedures makes this possible.

Other Jurisdictions
A good recent example of the power to control procedure can be found in the recent amendments to Saskatchewan's law.[85]

Recommendation #27: Power to determine procedure
Amend s. 38 of *FOIPOP* and s. 491 of the *MGA* to add general powers of the Commissioner that include the power to determine the procedure to be followed in the exercise of the powers or performance of any duties pursuant to the *MGA* or *FOIPOP*.

E. iii b Power to Compel Production of Records

Problem
The Commissioner currently has the authority to require production of records. There are three shortcomings with this power: records over which solicitor-client privilege is claimed, the scope of the power to demand production, and return of records at the end of a review.

Recently, Canadian courts have made clear that in order for oversight bodies such as Information and Privacy Commissioners to have the power to compel production of records over which solicitor-client privilege is claimed, the legislation must clearly indicate this authority.[86] *FOIPOP* and the *MGA* are worded in a manner that clearly states that the Commissioner has authority to demand production of records including records privileged at law. However, to properly protect these records it would be useful to have a provision that makes clear that the privilege is not affected by the disclosure to the Commissioner.

The second problem is that the right to compel production of records is limited to any record that is in the custody or under the control of a public body. When privacy breaches occur, third parties sometimes end up in possession of personal information to which they are not entitled. This occurs when faxes are misdirected or mail is directed to the wrong address, for example. An update in the authority to compel production in the custody or control of a public body or any other person would aid in the investigation of privacy breaches.

---

[84] Guide to OIPC NS Processes, August 2016 available at: https://foipop.ns.ca/sites/default/files/publications/Guide%20to%20OIPC%20NS%20Processes%20%2826%20August%2016%29.pdf.
[85] See Appendix 1 for this example.
[86] For example, the recent decision of the *Supreme Court of Canada in Alberta (Information and Privacy Commissioner) v. University of Calgary,* 2016 SCC 53.

The third problem relating to the power to compel production is that *FOIPOP* is not clear what the Commissioner should do with the record upon the conclusion of the matter. It is the current practice of the OIPC to either return responsive records upon request or, securely destroy them upon resolution of a file.

Other Jurisdictions
British Columbia's access law is a good example of a production power that addresses all three problems outlined above.[87]

Recommendation #28: Power to compel production
Amend s. 38 of *FOIPOP* to:
a) Make clear that solicitor-client privilege is not affected by disclosure to the Commissioner.
b) Require any person to produce a record for the Commissioner that is in the person's custody or control, including personal information.
c) Require the Commissioner to return any record or copy of any record produced by the public body concerned.

E. iii c Information Sharing with Other Commissioners

Problem
Information sharing occurs not just within provincial entities but also across jurisdictions. In addition, public bodies and municipalities often use service providers from other jurisdictions. When breaches occur that involve service providers, the breach can affect other customers including government agencies in other jurisdictions. In other words, in the age of big data, privacy breaches know no borders. In order to effectively investigate such breaches the Commissioner requires the clear authority to work together with her regulatory counterparts to investigate these types of breaches and to co-ordinate activities to help prevent breaches.

Other Jurisdictions
Several jurisdictions across Canada have specific provisions that enable the Commissioner to share information for the purposes of conducting reviews, investigating complaints, or for other general monitoring purposes. Saskatchewan recently added these powers to its public sector law. British Columbia and Alberta have both had similar provisions for a number of years.[88]

Recommendation #29: Information sharing between oversight agencies
Amend *FOIPOP* and the *MGA* to allow the Commissioner to exchange information with extra-provincial Commissioners for the purpose of coordinating activities and handling reviews and complaints involving two or more jurisdictions.

E. iii d Grounds to Refuse to Conduct or Continue a Review

Problem
The laws as currently written state that the Commissioner, on completing a review, must complete a written report. There are a number of common reasons why proceeding to a written report would not serve the purposes of the Acts. More modern access to information and privacy statutes have incorporated a number of these grounds to refuse to conduct or continue a review.

[87] See Appendix 1 for a copy of s. 44 of the BC Commissioner's power to compel production.
[88] Examples of information sharing authorities between Commissioner's offices can be found in Appendix 1.

Nova Scotia's *Personal Health Information Act* contains a provision permitting the Commissioner to decide not to conduct a review in a number of circumstances including because the custodian has adequately responded to the concerns, passage of time, or because the review is frivolous or vexatious.[89]

Other Jurisdictions
Saskatchewan's public sector access law includes a number of grounds upon which the Commissioner may discontinue the review. Recent amendments to the law added a number of other grounds. Likewise the recent amendments to Newfoundland's law include a list of grounds that permit the Commissioner, at any stage of an investigation, to refuse to investigate a complaint.[90] Additional grounds to refuse to proceed are because the application for review concerns a trivial matter, was not made in good faith or does not contain sufficient evidence.

Recommendation #30: Grounds to refuse to proceed with a review
a) Amend *FOIPOP* and the *MGA* to add a provision that states that where the Commissioner is satisfied that there are reasonable grounds to review any matter, the Commissioner shall review the matter. Include grounds where the Commissioner may refuse to conduct a review including where the application is frivolous or vexatious, not made in good faith, concerns a trivial matter, does not contain sufficient evidence, has already been the subject of a report by the Commissioner, the public body has responded adequately to the complaint, the length of time that has elapsed, or for any other reason it is fair and reasonable not to conduct a review.
b) Amend s. 39 of *FOIPOP* and s. 492 of the *MGA* to provide that on completing a review the Commissioner "may" prepare a written report rather than "shall" prepare a written report.

E. iii e Time Limits on Commissioner's Processes

Problem
The Office of the Information and Privacy Commissioner has a backlog of cases. By 2014 there were unresolved cases dating back to 2009. Following a change in the case management strategy of the office, the backlog has slowly been reduced. At the current pace, by mid-2018 the Commissioner's office expects to be assigning 2017 files for investigation.

Part of the challenge for the Commissioner's office is that public bodies often require extra time to manage review files because of their limited resources. This can and does add months to the resolution process. In combination with a shift in the burden to comply with recommendations, a time limit on the Commissioner to resolve cases will encourage public bodies to properly resource their access and privacy groups so that they can actively participate in the resolution process. Failure to do so could lead to a recommendation with which they must comply unless they get approval from the court. In this context, imposing a time limit on the Commissioner makes sense.

A second challenge in terms of imposing a time limit on the Commissioner's office is the level of resourcing currently provided to the OIPC. The caseload at the OIPC has more than doubled since 2013.[91] In addition, in the spring of 2013, the Commissioner was given additional oversight responsibilities under the *Personal Health Information Act.* The increase in the caseload does not

[89] *Personal Health Information Act*, s. 95. Copy available in Appendix 1.
[90] Copies of the Saskatchewan and Newfoundland provisions are available in Appendix 1.
[91] In 2013 we received a total of 182 new review requests and opened 45 new outreach files for a total of 227 new matters. In 2016/17 we received a total of 371 new files plus 178 outreach files for a total of 549 new matters.

include the new responsibility to receive breach reports and reports of disclosures without consent to researchers. These reports have increased from 10 in 2013 to 815 in 2016/17.[92] Effective April 2017, the OIPC received the resources to staff one senior investigator position focusing on health privacy law. While this will help address the *PHIA* caseload, the steadily growing *FOIPOP* and *MGA* caseload will continue to be a challenge for meeting any hard timelines.

A properly resourced OIPC should provide services within a reasonable amount of time. Once a case is assigned to an investigator, on average, informal resolutions take 60 days. There will be occasions when a longer period of time can be very fruitful and other cases take only a few days to resolve. The best resolution is a resolution reached by agreement between the parties and sometimes this takes more time, especially if the matter includes third party interests. If the matter does not resolve during the informal resolution stage then additional time is required to allow the parties to provide written submissions (usually two to three weeks) and then to allow the Commissioner time to complete a written review report (usually four to eight weeks depending on the complexity of the issues).

Other Jurisdictions

There are a variety of approaches to timelines in Commissioners' offices across Canada. Most offices report a backlog of cases whether or not they have statutory timelines. British Columbia has a 90 day review timeline with an authority for the Commissioner to extend the date with notice to the parties.

Newfoundland's new law sets a strict 65 day time limit for completion of reviews by the Newfoundland Commissioner. In order to extend the timeline, the Commissioner in Newfoundland must apply to the court.

A 65 day time limit would not work for the OIPC in Nova Scotia at its current resource level. The OIPC in Newfoundland has 13 staff plus the Commissioner, the OIPC in Nova Scotia has six staff plus the Commissioner.[93] It is a challenge to meet the 65 day timeline with 13 staff, it would be impossible with only 6. Significant additional resources would have to be added to the OIPC. Further, under Newfoundland's law, the Commissioner must seek court approval to extent the 65 day timeline. The addition of a requirement that the Commissioner apply to court to extend the time would add both costs and time to the OIPC processes.

It makes more practical sense to write into the law the circumstances under which the Commissioner herself may extend any imposed time limit.

Recommendation #31: Review and complaint time limits

Amend *FOIPOP* and the *MGA* to provide that the Commissioner should conclude her investigation and mediation processes and, if necessary, issue a report within 90 days of receipt of a complaint or request for review. Include an option to allow for longer period of time at the Commissioner's discretion and with written notice to the parties.

---

[92] The *Personal Health Information Act* came into effect on June 1, 2013 and requires that health custodians report minor privacy breaches and any disclosures without consent to researchers. These numbers reflect those reports but the OIPC has not been given any additional resources to manage a thorough review of this information.

[93] According to the Newfoundland OIPC's 2015/16 Annual Report, the Office employs 13 staff and the Commissioner. Available at http://www.oipc.nl.ca/pdfs/OIPC%20annual%20report%202015-2016.pdf). In 2015/16 the OIPC Nova Scotia had five staff plus the Commissioner, rising to six in fiscal year 2017/18.

E. iv General Powers of the Commissioner

Problem

Currently the Commissioner's powers with respect to the access provisions are vastly differently from her powers with respect to compliance with the privacy provisions. Many of the provisions missing from the Commissioner's access powers are provisions that allow the Commissioner to act proactively through education and through providing comment to public bodies and municipalities. Nova Scotia has many small public bodies and municipalities who receive very few access to information requests. As a result, there is a lack of training and experience in most of these organizations. The Office of the Information and Privacy Commissioner is an office consisting of independent access and privacy experts who can provide information, education, guidance, and leadership. Allowing the OIPC to provide the same leadership on access issues that it provides on privacy issues takes full advantage of an existing resource that benefits public bodies, municipalities, and citizens.

Nova Scotia's access and privacy laws also fail to provide the Commissioner with several other key powers including the power to initiate access-related investigations, conduct audits, comment on draft legislation (discussed earlier), and comment on the privacy implications of new automated systems and data linking proposals. Such powers would ensure that systemic problems, for example chronic delays, inconsistent fees, and failure to meet the duty to assist, could all be the subject of effective independent oversight with the use of an auditing power or self-initiated investigations.

Other Jurisdictions

Other jurisdictions are considering similar modernization of Commissioner's powers. For example, the Privacy Commissioner of Canada has recommended that the Office of the Privacy Commissioner be given an explicit education and research mandate as well as the authority to comment on the privacy implications of new legislation.[94] Saskatchewan's recent amendments included additional general powers for the Commissioner. In other jurisdictions such as British Columbia, the public sector access law already provides broad general powers for the Commissioner for both access and privacy related matters.

Recommendation # 32: General powers of Commissioner

Amend s. 38 of *FOIPOP* and s. 491 of the *MGA* to add general powers of the Commissioner that include the following:

a) Monitor how the privacy and access provisions are administered and conduct reviews of access and privacy complaints arising from the access and privacy provisions.
b) Initiate investigations of access and privacy compliance including matters or allegations of unauthorized destruction of records.
c) Make recommendations on and mediate access and privacy complaints.
d) Undertake research matters concerning privacy and access legislation.
e) Inform the public about the Acts.
f) Conduct audits.
g) Authorize public bodies and municipalities to disregard requests.
h) Determine OIPC procedures.
i) Comment on the implications for access to information or for protection of privacy of any matter including proposed projects, activities, systems, information sharing agreements and legislative schemes of public bodies and municipal bodies.

[94] *Privacy Act Reform* at p. 9.

F. Offences

Problem

Nova Scotia's laws contain the weakest offence provisions in Canada both in terms of their scope and their consequences. In Nova Scotia there are only two offences:

- Maliciously collecting or disclosing personal information in contravention of *FOIPOP* (s. 47) or the *MGA* (s. 500).
- Knowingly altering a record that is subject to a request in order to mislead the person who made the request (s. 47(1A) of *FOIPOP* and s. 500 (1A) of *MGA*).

On conviction of either offence the person is subject to a fine of not more than two thousand dollars or imprisonment for six months, or both.

The offences fail to protect Nova Scotians against the unauthorized collection, use, or disclosure of their personal information. They fail to adequately ensure that the integrity of the appeal process is protected, and they fail to adequately punish offenders in a manner that could reasonably be expected to deter others.

Other Jurisdictions

Other jurisdictions in Canada include the following types of offences in their access and privacy laws:

- Obstructing the Commissioner (all jurisdictions[95] except Nova Scotia).
- Misleading the Commissioner and knowingly making a false statement to the Commissioner (Alberta, British Columbia, Manitoba, Newfoundland, Northwest Territories, Yukon, Saskatchewan, PEI).
- Obstructing the right of access, destroying, altering, falsifying, or concealing a record with intent to evade a request for access (Canada, Manitoba, New Brunswick, Newfoundland, Ontario, PEI, Yukon).
- Directing another to destroy, alter, falsify, or conceal any record (PEI, Newfoundland, New Brunswick).
- Willfully or knowingly collecting, using, or disclosing personal information in contravention of the law (PEI, Ontario, Saskatchewan, Newfoundland, New Brunswick, Manitoba, British Columbia, Alberta).

[95] The offence provisions are as follows: *Access to Information Act*, RSC 1985 c A-1, s. 67, *Privacy Act* RSC 1985 c. P-21 s. 68, *Freedom of Information and Protection of Privacy Act* (Alberta) RSA 200, c F-25, s. 92, *Freedom of Information and Protection of Privacy Act* (British Columbia) RSBC 1996 c. 165, s. 74, 74.1, *Freedom of Information and Protection of Privacy Act* (Manitoba), CCSM c. F175, s. 85, s. 86, *Right to Information and Protection of Privacy Act* (New Brunswick), SNB 2009 c R-10.6, s. 82, *Right to Information and Protection of Privacy Act 2015* (Newfoundland and Labrador), SNL 2015, c A-1.2, s. 115, *Access to Information and Protection of Privacy Act* (Northwest Territories) SNWT 1994 c. 20 s. 59, *Freedom of Information and Protection of Privacy Ac*t (Saskatchewan), SS 1990-91, c F-22.01, s. 68, *Freedom of Information and Protection of Privacy Act* (Ontario) RSO 1990 c F.31 s. 61, *Freedom of Information and Protection of Privacy Act* (PEI) RSPEI 1988, c F-15.01 s. 75, *Access to Information and Protection of Privacy Act* (Yukon) RSY 2002 c 1, s. 67.

The fines under other access and privacy laws are either higher than Nova Scotia's or have risen in recent years:

$1000	Canada, Saskatchewan
$2000	British Columbia (individuals)
$5000	Manitoba, Northwest Territories, Ontario, Yukon
$10,000	Alberta, Newfoundland, PEI
$25,000	British Columbia (partnership or service provider)
$500,000	British Columbia (corporations)

A number of recent reviews of access and privacy laws have recommended that fines be increased. For example, Canada's Information Commissioner recommends that fines be increased from $1,000 to $5,000 for obstructing the Commissioner and to $10,000 for destroying, mutilating, or altering a record with intent to deny a right of access.[96] The Special Committee of the legislature that recently reviewed British Columbia's access and privacy law recommended that fines for general offences be increased from $2,000 to $10,000 and that the maximum fines for privacy offences committed by individuals be increased to $25,000.[97] Saskatchewan currently has amendments before the House that include an increase in fines from $1,000 to $50,000.[98]

Taking into account the proposed fine increases in British Columbia, Saskatchewan, and at the federal level, the average fine provision in Canada is $15,000.

Recommendation #33: Update offence provisions

Update Nova Scotia's offence provisions by:

a) Making the following offences under the law:
- obstructing the Commissioner;
- misleading the Commissioner and knowingly making a false statement to the Commissioner;
- obstructing the right of access by destroying, altering, falsifying, or concealing a record with intent to evade a request for access;
- directing another to destroy, alter, falsify, or conceal any record; and
- willfully or knowingly collecting, using, or disclosing personal information in contravention of the law.

b) Set the fine on conviction at a maximum of $20,000 for individuals and higher for organizations and service providers.

[96] *Striking the Right Balance for Transparency* at p. 88.
[97] *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, May 2016 at p. 88.
[98] *An Act to amend the Freedom of Information and Protection of Privacy Act*, Bill No. 30, s. 30 (Sask).

G. Review of the Acts

Problem

FOIPOP only contemplated one review done in 2003. New technical, policy, and legislative developments can greatly impact privacy and access issues. When there is no requirement to periodically review access and privacy laws, the laws cannot remain current and relevant to modern realities and challenges. In addition, we should, whenever possible, harmonize data protection laws to ensure a consistent privacy regime across Canada.[99] Regular reviews of access and privacy laws is best practice, particularly in a world where new technologies create new opportunities and new challenges for access and privacy rights.

Other Jurisdictions

A review of provisions across Canada reveals the following characteristics of statutory review provisions:

- Review periods range between five and six years.
- Legislation calls for a comprehensive review.
- Review is conducted by a special committee of the legislature.
- Submissions are published online by the committee.
- Reports are completed within one and one and a half years and in practice, are made public.

Recommendation #34: Review of the Acts

Amend s. 50 of *FOIPOP* and add provisions to *PRO*, *PIIDPA* and the *MGA* to require that:

a) A review must be conducted of each Act at least every six years.
b) The reviews must be conducted by an independent committee of the legislature.
c) All submissions and reports of the committee must be made public.
d) Each review must include a mandatory review of any and all notwithstanding clauses and a review of s. 4A(2) of *FOIPOP* and s. 464A(2) of the *MGA*.

[99] The Privacy Commissioner of Canada made a similar point in his submission to the ETHI Committee – *Privacy Act Reform in an Era of Change and Transparency* at p. 9.

Appendix 1: Sample Statutory Provisions

Modernizing Access Rights

B. ii Extending Coverage

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

> 3 (2) Clause 2(2)(b) is repealed and the following substituted:
> "(b) the Legislative Assembly Service or, subject to subsections 3(3) and (4), offices of members of the Assembly or members of the Executive Council".
>
> Repealed clause 2(2)(b) read:
> (2) "Government institution" does not include:
> (b) the Legislative Assembly Service or offices of members of the Executive Council;

New subsections 3(3) and (4) provide:

> The following subsections are added after subsection 3(2):
> "(3) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Assembly and their employees as if the members and their offices were government institutions:
> (a) sections 24 to 30;
> (b) section 33.
>
> "(4) Subject to the regulations, the following sections apply, with any necessary modification, to offices of members of the Executive Council and their employees as if the members and their offices were part of the government institution for which the member of the Executive Council serves as the head:
> (a) sections 24 and 24.1;
> (b) sections 25 to 30;
> (c) section 33".

Sections 24 to 30 and s. 33 referenced above are the protection of privacy rules in Saskatchewan's public sector privacy legislation.

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

> **Definitions**
> 2. In this Act
>
> (x) "public body" means
> (i) a department created under the *Executive Council Act* , or a branch of the executive government of the province,
> (ii) a corporation, the ownership of which, or a majority of the shares of which is vested in the Crown,
> (iii) a corporation, commission or body, the majority of the members of which, or the majority of members of the board of directors of which are appointed by an Act, the Lieutenant-Governor in Council or a minister,

(iv) a local public body,
(v) the House of Assembly and statutory offices, as defined in the *House of Assembly Accountability, Integrity and Administration Act*, and
(vi) a corporation or other entity owned by or created by or for a local government body or group of local government bodies, which has as its primary purpose the management of a local government asset or the discharge of a local government responsibility,

and includes a body designated for this purpose in the regulations made under section 116 , but does not include

(vii) the constituency office of a member of the House of Assembly wherever located,
(viii) the Court of Appeal, the Trial Division, or the Provincial Court , or
(ix) a body listed in Schedule B;

British Columbia – *Freedom of Information and Protection of Privacy Act* RSBC c. 165

3(3) The following sections apply to officers of the Legislature, their employees and, in relation to their service providers, the employees and associates of those service providers, as if the officers and their offices were public bodies:

(a) section 30 (protection of personal information);
(b) section 30.1 (storage and access must be in Canada);
(c) section 30.2 (obligation to report foreign demand for disclosure);
(d) section 30.3 (whistle-blower protection);
(e) section 30.4 (unauthorized disclosure prohibited);
(e.1) section 30.5 (notification of unauthorized disclosure);
(f) section 33 (disclosure of personal information);
(g) section 33.1 (disclosure inside or outside Canada);
(h) section 33.2 (disclosure inside Canada only);
(i) section 74.1 (privacy protection offences).

C. i Protecting Applicant Identity

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Anonymity

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

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

(a) respecting personal information about the applicant; or

Where the name of the applicant is necessary to respond to the request and the applicant has consented to its disclosure.

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

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

C. ii Fees

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Costs

25. (1) The head of a public body shall not charge an applicant for making an application for access to a record or for the services of identifying, retrieving, reviewing, severing or redacting a record.

(2) The head of a public body may charge an applicant a modest cost for locating a record only, after

(a) the first 10 hours of locating the record, where the request is made to a local government body; or

(b) the first 15 hours of locating the record, where the request is made to another public body.

(3) The head of a public body may require an applicant to pay

(a) a modest cost for copying or printing a record, where the record is to be provided in hard copy form;

(b) the actual cost of reproducing or providing a record that cannot be reproduced or printed on conventional equipment then in use by the public body; and

(c) the actual cost of shipping a record using the method chosen by the applicant.

(4) Notwithstanding subsections (2) and (3), the head of the public body shall not charge an applicant a cost for a service in response to a request for access to the personal information of the applicant.

(5) The cost charged for services under this section shall not exceed either

(a) the estimate given to the applicant under section 26; or

(b) the actual cost of the services.

(6) The minister responsible for the administration of this Act may set the amount of a cost that may be charged under this section.

C. iii Format of Records

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Provision of information

20(2) Where the requested information is in electronic form in the custody or under the control of a public body, the head of the public body shall produce a record for the applicant where

a) It can be produced using the normal computer hardware and software and technical expertise of the public body; and

b) Producing it would not interfere unreasonably with the operations of the public body.

(3) Where the requested information is information in electronic form that is, or forms part of, a dataset in the custody or under the control of a public body, the head of the public body

shall produce the information for the applicant in an electronic form that is capable of re-use where

a) it can be produced using the normal computer hardware and software and technical expertise of the public body;
b) producing it would not interfere unreasonably with the operations of the public body; and
c) it is reasonably practicable to do so.

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

Manner of access

10(1) If an applicant is entitled to access pursuant to subsection 9(1), a head shall provide the applicant with access to the record in accordance with this section.

(2) Subject to subsection (3), if a record is in electronic form, a head shall give access to the record in electronic form if:

(a) it can be produced using the normal computer hardware and software and technical expertise of the government institution;

(b) producing it would not interfere unreasonably with the operations of the government institution; and

(c) it is reasonably practicable to do so.

(3) If a record is a microfilm, film, sound or video recording or machine-readable record, a head may give access to the record:

(a) by permitting the applicant to examine a transcript of the record;

(b) by providing the applicant with a copy of the transcript of the record; or

(c) in the case of a record produced for visual or aural reception, by permitting the applicant to view or hear the record or by providing the applicant with a copy of it.

C. v Modernizing Exemptions

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

Schedule 1 - Definitions

"personal information" means recorded information about an identifiable individual other than contact information;

"contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;

C. vii Disregarding a Request

Nova Scotia – *Personal Health Information Act* SN 2010, c 41

81 (1) Where a custodian believes on reasonable grounds that a request for access

a) Is frivolous or vexatious; or
b) Is part of a pattern of conduct that amounts to an abuse of the right of access,

The custodian may refuse to grant the request.

89 Where a custodian believes on reasonable grounds that a request for a correction
a) Is frivolous or vexatious; or
b) Is part of a pattern of conduct that amounts to an abuse of the right of correction,
The custodian may refuse to grant the request and shall provide written notice to the individual.

New Brunswick – *Right to Information and Protection of Privacy Act* S.N.B. 2009, c. R-10.6

15 On the request of a public body, the Commissioner may authorize the head to disregard one or more requests for access if the request for access:
a) Would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the request or previous requests;
b) Is incomprehensible, frivolous or vexatious or
c) Is for information already provided to the applicant.

British Columbia – *Freedom of Information and Protection of Privacy Act* RSBC c. 165

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.

Northwest Territories and Nunavut – *Access to Information and Protection of Privacy Act* S.N.W.T. 1994 c. 20

53 The Information and Privacy Commissioner may, at the request of the head of a public body, authorize the public body to disregard a request under section 6 that
a) Is frivolous or vexatious;
b) Is not made in good faith
c) Concerns a trivial matter;
d) Amounts to an abuse of the right to access; or
e) Would unreasonably interfere with the operations of the public body because of its repetitious or systematic nature.

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Disregarding a request
21. (1) The head of a public body may, not later than 5 business days after receiving a request, apply to the commissioner for approval to disregard the request where the head is of the opinion that
(a) the request would unreasonably interfere with the operations of the public body;
(b) the request is for information already provided to the applicant; or
(c) the request would amount to an abuse of the right to make a request because it is
(i) trivial, frivolous or vexatious,
(ii) unduly repetitive or systematic,
(iii) excessively broad or incomprehensible, or
(iv) otherwise made in bad faith.

(2) The commissioner shall, without delay and in any event not later than 3 business days after receiving an application, decide to approve or disapprove the application.
(3) The time to make an application and receive a decision from the commissioner does not suspend the period of time referred to in subsection 16 (1).
(4) Where the commissioner does not approve the application, the head of the public body shall respond to the request in the manner required by this Act.
(5) Where the commissioner approves the application, the head of a public body who refuses to give access to a record or correct personal information under this section shall notify the person who made the request.
(6) The notice shall contain the following information:

a) that the request is refused because the head of the public body is of the opinion that the request falls under subsection (1) and of the reasons for the refusal;
b) that the commissioner has approved the decision of the head of a public body to disregard the request; and
c) that the person who made the request may appeal the decision of the head of the public body to the Trial Division under subsection 52 (1).

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

Power to authorize a government institution to disregard applications or requests
45.1
(1) The head may apply to the commissioner to disregard one or more applications pursuant to section 6 or requests pursuant to section 32.
(2) In determining whether to grant an application or request mentioned in subsection (1), the commissioner shall consider whether the application or request:

(a) would unreasonably interfere with the operations of the government institution because of the repetitious or systematic nature of the application or request;
(b) would amount to an abuse of the right of access or right of correction because of the repetitious or systematic nature of the application or request; or
(c) is frivolous or vexatious, not in good faith or concerns a trivial matter.

(3) The application pursuant to subsection 6(1) or the request pursuant to clause 32(1)(a) is suspended until the commissioner notifies the head of the commissioner's decision with respect to an application or request mentioned in subsection (1).
(4) If the commissioner grants an application or request mentioned in subsection (1), the application pursuant to subsection 6(1) or the request pursuant to clause 32(1)(a) is deemed to not have been made.
(5) If the commissioner refuses an application or request mentioned in subsection (1), the 30-day period mentioned in subsection 7(2) or subsection 32(2) resumes".

C. viii Open Data and Open Government

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Publication scheme

111. (1) The commissioner shall create a standard template for the publication of information by public bodies to assist in identifying and locating records in the custody or under the control of public bodies.

(2) The head of a public body shall adapt the standard template to its functions and publish its own information according to that adapted template.

(3) The published information shall include

(a) a description of the mandate and functions of the public body and its components;

(b) a description and list of the records in the custody or under the control of the public body, including personal information banks;

(c) the name, title, business address and business telephone number of the head and coordinator of the public body; and

(d) a description of the manuals used by employees of the public body in administering or carrying out the programs and activities of the public body.

(4) The published information shall include for each personal information bank maintained by a public body

(a) its name and location;

(b) a description of the kind of personal information and the categories of individuals whose personal information is included;

(c) the authority and purposes for collecting the personal information;

(d) the purposes for which the personal information is used or disclosed; and

(e) the categories of persons who use the personal information or to whom it is disclosed.

(5) Where personal information is used or disclosed by a public body for a purpose that is not included in the information published under subsection (2), the head of the public body shall

(a) keep a record of the purpose and either attach or link the record to the personal information; and

(b) update the published information to include that purpose.

Report of Minister Responsible

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

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

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

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

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

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

C. ix Mandatory Public Interest Override

Type 1:

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

Section 25 provides in part:

> 25 (1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people or to an applicant, information
>
> (a) about a risk of significant harm to the environment or to the health or safety of the public or a group of people, or
>
> (b) the disclosure of which is, for any other reason, clearly in the public interest.

Alberta – *Freedom of Information and Protection of Privacy Act* S.A. 2003, c. P-6.5

Section 32 provides in part:

> 32(1) Whether or not a request for access is made, the head of a public body must, without delay, disclose to the public, to an affected group of people, to any person or to an applicant
>
> (a) information about a risk of significant harm to the environment or to the health or safety of the public, of the affected group of people, of the person or of the applicant, or
>
> (b) information the disclosure of which is, for any other reason, clearly in the public interest.
>
> (2) Subsection (1) applies despite any other provision of this Act.

Ontario – *Freedom of Information and Protection of Privacy Act* R.S.O. 1990 c. F-31

Section 11 provides in part:

> 11. (1) Despite any other provision of this Act, a head shall, as soon as practicable, disclose any record to the public or persons affected if the head has reasonable and probable grounds to believe that it is in the public interest to do so and that the record reveals a grave environmental, health or safety hazard to the public.

Type 2:

Ontario – *Freedom of Information and Protection of Privacy Act* R.S.O. 1990, c. F-31

> **Exemptions not to apply**
>
> 23. An exemption from disclosure of a record under sections 13, 15, 17, 18, 20, 21 and 21.1 does not apply where a compelling public interest in the disclosure of the record clearly outweighs the purpose of the exemption. R.S.O. 1990, c. F.31, s. 23; 1997, c. 41, s. 118 (2).

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

> **Public interest**
>
> 9. (1) Where the head of a public body may refuse to disclose information to an applicant under a provision listed in subsection (2), that discretionary exception shall not apply

where it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception.

(2) Subsection (1) applies to the following sections:

(a) section 28 (local public body confidences);

(b) section 29 (policy advice or recommendations);

(c) subsection 30 (1) (legal advice);

(d) section 32 (confidential evaluations);

(e) section 34 (disclosure harmful to intergovernmental relations or negotiations);

(f) section 35 (disclosure harmful to the financial or economic interests of a public body);

(g) section 36 (disclosure harmful to conservation); and

(h) section 38 (disclosure harmful to labour relations interests of public body as employer).

(3) Whether or not a request for access is made, the head of a public body shall, without delay, disclose to the public, to an affected group of people or to an applicant, information about a risk of significant harm to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.

(4) Subsection (3) applies notwithstanding a provision of this Act.

Modernizing Privacy Rights

D. i Standards for Sharing Personal Information

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

33.1 (1) A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

(e) to an individual who is a minister, an officer of the public body or an employee of the public body other than a service provider, if

(i) the information is necessary for the performance of the duties of the minister, officer or employee, and

(ii) in relation to disclosure outside Canada, the outside disclosure is necessary because the individual is temporarily travelling outside Canada;

(e.1) to an individual who is a service provider of the public body, or an employee or associate of such a service provider, if

(i) the information is necessary for the performance of the duties of the individual in relation to the public body, and

(ii) in relation to disclosure outside Canada,

(A) the individual normally receives such disclosure only inside Canada for the purpose of performing those duties, and

(B) the outside disclosure is necessary because the individual is temporarily travelling outside Canada;

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

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

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

Ontario – *Freedom of Information and Protection of Privacy Act* R.S.O. 1990 c. F-31

42. (1) An institution shall not disclose personal information in its custody or under its control except,

(d) where disclosure is made to an officer, employee, consultant or agent of the institution who needs the record in the performance of their duties and where disclosure is necessary and proper in the discharge of the institution's functions;

Common or integrated program or activity:

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

33.2 A public body may disclose personal information referred to in section 33 inside Canada as follows:

(d) to an officer or employee of

(i) a public body, or

(ii) an agency,

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

Schedule 1

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

(a) provides one or more services through

(i) a public body and one or more other public bodies or agencies working collaboratively, or

(ii) one public body working on behalf of one or more other public bodies or agencies, and

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

69 (5.2) If the minister responsible for this Act receives a privacy impact assessment under subsection (5.1) respecting a common or integrated program or activity or a data-linking initiative, the minister must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the commissioner for the commissioner's review and comment.

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

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

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

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

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

New Brunswick – *Right to Information and Protection of Privacy Act* SNB 2009, c. R-10.6

46(1) A public body may disclose personal information only

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

Provincial identity information service provider:

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

Purpose for which personal information may be collected

26 A public body may collect personal information only if

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

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

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

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

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

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

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

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

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

(i) at which the individual voluntarily appears, and

(ii) that is open to the public, or

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

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

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

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

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

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

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

(a) identifying an individual;
(b) verifying the identity of an individual;
(c) updating personal identity information about an individual;
(d) issuing a physical or an electronic credential to an individual;
(e) managing the information associated with a physical or an electronic credential;
(f) any other service related to personal identity information that the minister responsible for this Act considers appropriate.

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

(a) the type and quantity of personal identity information required to identify, or verify the identity of, individuals seeking access to government services,
(b) the provision to individuals of physical and electronic credentials for use in accessing government services,
(c) the privacy and security of personal identity information that is collected, used or disclosed under this Act,
(d) the format in which personal identity information is collected, used or disclosed under this Act, and
(e) the circumstances in which particular types of personal identity information may or may not be collected, used or disclosed in relation to services provided under subsection (2).

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

D. ii a Core Privacy Standards

Nova Scotia – *Personal Health Information Act*, SNS 2010 c. 41

24 A custodian shall not collect, use or disclose personal health information if other information will serve the purpose of the collection, use or disclosure.

25 (1) The collection, use and disclosure of personal health information must be limited to the minimum amount of personal health information necessary to achieve the purpose for which it is collected, used and disclosed.

(2) For greater certainty,

(a) in respect of the use of personal health information by a custodian, the custodian shall limit the use of personal health information in its custody or under its control to those of its agents who need to know the information to carry out the purpose for which the information was collected or a purpose authorized under this Act; and
(b) in respect of the disclosure of personal health information by a custodian, the custodian shall limit the disclosure of personal health information in the custodian's custody or under the custodian's control to those regulated health professionals, who have the right to treat individuals in the custodian's health care facility, to only that information that the health professionals require to carry out their duties and responsibilities.

D. ii b Mandatory Privacy Impact Assessments

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

> 69 (5) The head of a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for this Act.
>
> (5.1) The head of a ministry, with respect to a proposed enactment, system, project, program or activity, must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the minister responsible for this Act for the minister's review and comment.
>
> (5.2) If the minister responsible for this Act receives a privacy impact assessment under subsection (5.1) respecting a common or integrated program or activity or a data-linking initiative, the minister must submit, during the development of the proposed enactment, system, project, program or activity, the privacy impact assessment to the commissioner for the commissioner's review and comment.
>
> (5.3) The head of a public body that is not a ministry must conduct a privacy impact assessment in accordance with the directions of the minister responsible for this Act.
>
> (5.4) The head of a public body that is not a ministry, with respect to a proposed system, project, program or activity, must submit, during the development of the proposed system, project, program or activity, the privacy impact assessment, if it addresses a common or integrated program or activity or a data-linking initiative, to the commissioner for the commissioner's review and comment.
>
> (5.5) The head of a public body must notify the commissioner of a data-linking initiative or of a common or integrated program or activity at an early stage of developing the initiative, program or activity.

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

> **Privacy impact assessment**
> 72. (1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act
>
> (a) a privacy impact assessment for that minister's review and comment; or
> (b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.
>
> (2) A minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.
> (3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.
> (4) Where the minister responsible for this Act receives a privacy impact assessment respecting a common or integrated program or service for which disclosure of personal information may be permitted under paragraph 68 (1)(u), the minister shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.

D. ii c Information Sharing Agreements

Ontario – *Freedom of Information and Protection of Privacy Act* R.S.O. 1990 c. F-31

Service provider organizations
65.1 (1) This section applies with respect to a service provider organization as defined in section 17.1 of the *Ministry of Government Services Act*. 2006, c. 34, Sched. F, s. 1 (2).

Collection of personal information under arrangements
(7) A person who provides services on behalf of a service provider organization pursuant to an arrangement under subsection 17.1 (7) of the *Ministry of Government Services Act* may not collect personal information in connection with providing those services unless the service provider organization and the person have entered into an agreement that governs the collection, use and disclosure of such personal information and the agreement meets the prescribed requirements, if any. 2006, c. 34, Sched. F, s. 1 (2).

(9) The Lieutenant Governor in Council may make regulations,
(e) prescribing requirements for agreements under subsection (7);

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

69 (1) In this section:
"information-sharing agreement" means an agreement between a public body and one or more of the following:
(a) another public body;
(b) a government institution subject to the *Privacy Act* (Canada);
(c) an organization subject to the *Personal Information Protection Act* or the *Personal Information Protection and Electronic Documents Act* (Canada);
(d) a public body, government institution or institution as defined in applicable provincial legislation having the same effect as this Act;
(e) a person or a group of persons;
(f) a prescribed entity,
that sets conditions on the collection, use or disclosure of personal information by the parties to the agreement;

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

D. ii e Mandatory Breach Notification

New Brunswick – *Personal Health Information Privacy and Access Act*, s. 49(1)(c) and 49(2)

- Notify the individual and the commissioner at the first reasonable opportunity if
  - personal health information is stolen, lost, disposed of or disclosed to or accessed by an unauthorized person.
- Unless the custodian reasonably believes that the event will not have an adverse impact on the provision of health care, the individual or will not lead to the identification of the individual.
- Regulations include information that must be provided.

Newfoundland and Labrador – *Personal Health Information Act,* SNL 2008, s. 15(4)

- Where the custodian reasonably believes there has been a material breach as defined in the regulations the custodian shall inform the commissioner.
- Commissioner may recommend that the custodian notify the individual in certain circumstances (s. 15(5)).
- "material breach" – factors relevant in determining what constitutes a material breach include sensitivity, number of people, whether the custodian reasonably believes that the personal health information involved has been or will be misused and whether the cause of the breach or the pattern of breaches indicates a systemic problem.

Alberta – *Personal Information Protection Act*, S.A. 2003 c. P-6.5

- Organization must notify the Commissioner without unreasonable delay where there a reasonable person would consider that there exists a real risk of significant harm (s. 34.1)
- Commissioner can require notification of individual where there is a real risk of significant harm (s. 37.1)
- Regulations include detailed list of content for notices

Canada – *Digital Privacy Act*, S.C. 2015 c. 32 requires organizations to:

- Notify individuals and the Privacy Commissioner as soon as feasible of any breach that poses a "real risk of significant harm"
- Notify any third party that the organization believes is in a position to mitigate the risk of harm
- Maintain a record of the data breach and make these records available to the Privacy Commissioner upon request
- Form and content of notification and identification of risk factors may form part of the regulation – consultations currently underway

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

> s. 29.1 A government institution shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the government institution if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

D. ii f Mandatory Consultation on Draft Legislation

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

> **General powers and duties of commissioner**
> 95
> (2) In addition to the commissioner's powers and duties under Parts II and III, the commissioner shall exercise and perform the following powers and duties:

(e) comment on the implications for access to information or for protection of privacy of proposed legislative schemes, programs or practices of public bodies;

Amendments to statutes and regulations

112. (1) A minister shall consult with the commissioner on a proposed Bill that could have implications for access to information or protection of privacy, as soon as possible before, and not later than, the date on which notice to introduce the Bill in the House of Assembly is given.

(2) The commissioner shall advise the minister as to whether the proposed Bill has implications for access to information or protection of privacy.

(3) The commissioner may comment publicly on a draft Bill any time after that draft Bill has been made public.

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

General powers of commissioner

42 (1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may

(f) comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs or activities of public bodies,

D. ii g Direct Collection and Notifications

Ontario – *Freedom of Information and Protection of Privacy Act,* R.S.O. 1990, c. F-31

39. (1) Personal information shall only be collected by an institution directly from the individual to whom the information relates unless,

(a) the individual authorizes another manner of collection;

(b) the personal information may be disclosed to the institution concerned under section 42 or under section 32 of the *Municipal Freedom of Information and Protection of Privacy Act*;

(c) the Commissioner has authorized the manner of collection under clause 59 (c);

(d) the information is in a report from a reporting agency in accordance with the *Consumer Reporting Act*;

(e) the information is collected for the purpose of determining suitability for an honour or award to recognize outstanding achievement or distinguished service;

(f) the information is collected for the purpose of the conduct of a proceeding or a possible proceeding before a court or tribunal;

(g) the information is collected for the purpose of law enforcement; or

(h) another manner of collection is authorized by or under a statute. R.S.O. 1990, c. F.31, s. 39 (1).

(2) Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection. R.S.O. 1990, c. F.31, s. 39 (2).

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

How personal information is to be collected

62. (1) A public body shall collect personal information directly from the individual the information is about unless

(a) another method of collection is authorized by
  (i) that individual
  (ii) the commissioner under paragraph 95 (1)(c), or
  (iii) an Act or regulation;
(b) the information may be disclosed to the public body under sections 68 to 71;
(c) the information is collected for the purpose of
  (i) determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary,
  (ii) an existing or anticipated proceeding before a court or a judicial or quasi-judicial tribunal,
  (iii) collecting a debt or fine or making a payment, or
  (iv) law enforcement; or
(d) collection of the information is in the interest of the individual and time or circumstances do not permit collection directly from the individual.

(2) A public body shall tell an individual from whom it collects personal information
(a) the purpose for collecting it;
(b) the legal authority for collecting it; and
(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

(3) Subsection (2) does not apply where
(a) the information is about law enforcement or anything referred to in subsection 31 (1) or (2); or
(b) in the opinion of the head of the public body, complying with it would
  (i) result in the collection of inaccurate information, or
  (ii) defeat the purpose or prejudice the use for which the information is collected.

D. ii h Personal Information Banks

Canada – *Privacy Act* R.S.C. 1985

Index of personal information

11 (1) The designated Minister shall cause to be published on a periodic basis not less frequently than once each year, an index of

(a) all personal information banks setting forth, in respect of each bank,
  (i) the identification and a description of the bank, the registration number assigned to it by the designated Minister pursuant to paragraph 71(1)(b)

and a description of the class of individuals to whom personal information contained in the bank relates,

(ii) the name of the government institution that has control of the bank,

(iii) the title and address of the appropriate officer to whom requests relating to personal information contained in the bank should be sent,

(iv) a statement of the purposes for which personal information in the bank was obtained or compiled and a statement of the uses consistent with those purposes for which the information is used or disclosed,

(v) a statement of the retention and disposal standards applied to personal information in the bank, and

(vi) an indication, where applicable, that the bank was designated as an exempt bank by an order under section 18 and the provision of section 21 or 22 on the basis of which the order was made; and

(b) all classes of personal information under the control of a government institution that are not contained in personal information banks, setting forth in respect of each class

(i) a description of the class in sufficient detail to facilitate the right of access under this Act, and

(ii) the title and address of the appropriate officer for each government institution to whom requests relating to personal information within the class should be sent.

Statement of uses and purposes

(2) The designated Minister may set forth in the index referred to in subsection (1) a statement of any of the uses and purposes, not included in the statements made pursuant to subparagraph (1)(a)(iv), for which personal information contained in any of the personal information banks referred to in the index is used or disclosed on a regular basis.

Index to be made available

(3) The designated Minister shall cause the index referred to in subsection (1) to be made available throughout Canada in conformity with the principle that every person is entitled to reasonable access to the index.

E. i Improving Oversight

E. i c Employees, Experts, and Support

Nova Scotia – *Auditor General Act*, SNS 2010, c. 33

Employees
9 Notwithstanding the Civil Service Act or the General Civil Service Regulations, the Auditor General shall

(a) appoint such persons as employees in the Office as the Auditor General considers necessary to perform the Auditor General's duties; and
(b) place them in such positions as the Auditor General considers appropriate under such classification ratings and at such rates of remuneration within those classification ratings established by the Public Service Commission as the Auditor General considers appropriate. *2010, c. 33, s. 9.*

Experts and support
10 (1) Notwithstanding any Government procurement rules or policies, the Auditor General may engage the services of such counsel, accountants or other professionals or experts to advise or assist the Auditor General in respect of matters as the Auditor General considers necessary to carry out the Auditor General's duties under this Act.

(2) Payments made to experts under this Section may be determined by the Auditor General and must be within the limits of the appropriations, including any additional appropriations, for the Office.

(3) The Office may engage in such activities within and outside the Province as the Auditor General considers appropriate to support the audit and accounting professions and to support effective audit or accountability in government. *2010, c. 33, s. 10.*

Nova Scotia – *Elections Act*, SNS 2011, c. 5

Chief Electoral Officer appoints and places employees
15 (1) Notwithstanding the Civil Service Act or the General Civil Service Regulations, the Chief Electoral Officer shall
(a) appoint such individuals as employees of Elections Nova Scotia as the Chief Electoral Officer considers necessary to perform the duties of the Chief Electoral Officer;
(b) place employees in such positions as the Chief Electoral Officer considers appropriate under such classification ratings and at such rates of remuneration within those classification ratings established by the Public Service Commission as the Chief Electoral Officer considers appropriate; and
(c) establish the qualifications for the Assistant Chief Electoral Officer and establish a fair process for hiring based on merit and a fair process for removal. 2011, c. 5 elections

(2) The Chief Electoral Officer may appoint on a temporary basis, such individuals as are necessary to enable the Chief Electoral Officer to perform the duties and functions of that office.

(3) The Civil Service Act does not apply to individuals appointed pursuant to subsection (2) and the Chief Electoral Officer may establish their remuneration and the other terms and conditions of their engagement. 2011, c. 5, s. 15.

Experts
16 (1) Notwithstanding any Government procurement rules or policies, the Chief Electoral Officer may engage the services of such counsel, accountants, auditors or other professionals or experts to advise or assist the Chief Electoral Officer in respect of matters as the Chief Electoral Officer considers necessary to carry out the Chief Electoral Officer's powers and duties under this Act.
(2) Payments made to experts under this Section may be determined by the Chief Electoral Officer and must be within the limits of the appropriations, including any additional appropriations, for Elections Nova Scotia.

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act,* 2015

Commissioner's staff
92. (1) The commissioner may, subject to the approval of the House of Assembly Management Commission, and in the manner provided by law, appoint those assistants and employees that he or she considers necessary to enable him or her to carry out his or her functions under this Act and the Personal Health Information Act .

(2) Persons employed under subsection (1) are members of the public service of the province.

Ontario – *Freedom of Information and Protection of Privacy Act*, R.S.O. 1990, c. F.31

Staff
8. (1) Subject to the approval of the Lieutenant Governor in Council, the Commissioner may employ mediators and any other officers and employees the Commissioner considers necessary for the efficient operation of the office and may determine their salary and remuneration and terms and conditions of employment. R.S.O. 1990, c. F.31, s. 8 (1).

British Columbia – *Freedom of Information and Protection of Privacy Act,* RSBC 1996, c. 165

Staff of commissioner
41 (1) The commissioner may appoint, in accordance with the Public Service Act, employees necessary to enable the commissioner to perform the duties of the office.
(2) The commissioner may retain any consultants, mediators or other persons and may establish their remuneration and other terms and conditions of their retainers.
(3) The Public Service Act does not apply in respect of a person retained under subsection (2).
(4) The commissioner may make a special report to the Legislative Assembly if, in the commissioner's opinion,
(a) the amounts and establishment provided for the office of commissioner in the estimates, or
(b) the services provided by the BC Public Service Agency are inadequate for fulfilling the duties of the office.

New Brunswick – *Right to Information and Protection of Privacy Act* SNB 2009, c. R-10.6

> **Staff of the Office of the Access to Information and Privacy Commissioner**
> 58(1) The Commissioner may appoint such assistants and employees as the Commissioner considers necessary for the efficient carrying out of the Commissioner's powers and duties under this Act.

Saskatchewan – *Freedom of Information and Protection of Privacy Act*, SS 1991 c. F 22.01

> **Staff of commissioner**
> 43(1) The commissioner may appoint the employees that are required in order to exercise the powers and perform the duties of the commissioner effectively.
> (2) The Public Service Superannuation Act and The Public Employees Pension Plan Act apply to the members of the staff of the commissioner.
> (3) Members of the staff of the commissioner are employees of the Legislative Assembly and are not members of the public service of Saskatchewan.
> (4) The employee benefits applicable to the public servants of Saskatchewan apply or continue to apply, as the case may be, to the staff of the commissioner's office.
> (5) The commissioner shall:
> (a) administer, manage and control the commissioner's office and the general business of the office; and
> (b) oversee and direct the staff of the commissioner's office. 2015, c.16, s.4.

Prince Edward Island – *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01

> **Services**
> 48(2) The Commissioner may engage the services of any persons necessary to assist the Commissioner in carrying out the Commissioner's functions.

Delegation examples:

New Brunswick – *Right to Information and Protection of Privacy Act* SNB 2009, c. R-10.6

> Delegation of powers
> 59(1) The Commissioner may delegate, in writing, to any person any power of the Commissioner under this Act, except the power of delegation and the power to make a report under this Act.
> 59(2) Despite subsection (1), if the Commissioner is in a conflict of interest with respect to a matter referred to the Commissioner, the Commissioner may delegate in writing to any person any power with respect to that matter, including the power to make a report.
> 59(3) A person purporting to exercise a power of the Commissioner by virtue of a delegation under subsection (1) or (2) shall produce evidence of his or her authority to exercise that power when required to do so.
> 59(4) The Lieutenant-Governor in Council may prescribe by regulation circumstances that give rise to a conflict of interest for the purposes of subsection (2).

Newfoundland and Laborador – *Access to Information and Protection of Privacy Act* , 2015 SNL 2015, Chapter A-1.2

Delegation
103. The commissioner may delegate to a person on his or her staff a duty or power under this Act.

E. i d Restrictions on Disclosure and Immunity

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Disclosure of information
102. (1) The commissioner and a person acting for or under the direction of the commissioner, shall not disclose information obtained in performing duties or exercising powers under this Act, except as provided in subsections (2) to (5).
(2) The commissioner may disclose, or may authorize a person acting for or under his or her direction to disclose, information that is necessary to
(a) perform a duty or exercise a power of the commissioner under this Act; or
(b) establish the grounds for findings and recommendations contained in a report under this Act.
(3) In conducting an investigation and in performing a duty or exercising a power under this Act, the commissioner and a person acting for or under his or her direction, shall take reasonable precautions to avoid disclosing and shall not disclose
(a) any information or other material if the nature of the information or material could justify a refusal by a head of a public body to give access to a record or part of a record; or
(b) the existence of information, where the head of a public body is authorized to refuse to confirm or deny that the information exists under subsection 17 (2).
(4) The commissioner may disclose to the Attorney General information relating to the commission of an offence under this or another Act of the province or Canada, where the commissioner has reason to believe an offence has been committed.
(5) The commissioner may disclose, or may authorize a person acting for or under his or her direction to disclose, information in the course of a prosecution or another matter before a court referred to in subsection 99 (1).

Protection from liability
104. An action does not lie against the commissioner or against a person employed under him or her for anything he or she may do or report or say in the course of the exercise or performance, or intended exercise or performance, of his or her functions and duties under this Act, unless it is shown he or she acted in bad faith.

British Columbia – *Freedom of Information and Protection of Privacy Act* RSBC c. 165

Restrictions on disclosure of information by the commissioner and staff

47 (1) The commissioner and anyone acting for or under the direction of the commissioner must not disclose any information obtained in performing their duties, powers and functions under this Act, except as provided in subsections (2) to (5).

(2) The commissioner may disclose, or may authorize anyone acting on behalf of or under the direction of the commissioner to disclose, information that is necessary to

(a) conduct an investigation, audit or inquiry under this Act, or

(b) establish the grounds for findings and recommendations contained in a report under this Act.

(2.1) The commissioner and anyone acting for or under the direction of the commissioner must not give or be compelled to give evidence in court or in any other proceedings in respect of any records or information obtained in performing their duties or exercising their powers and functions under this Act.

(2.2) Despite subsection (2.1), the commissioner and anyone acting for or under the direction of the commissioner may give or be compelled to give evidence

(a) in a prosecution for perjury in respect of sworn testimony,

(b) in a prosecution for an offence under this Act,

(c) in an investigation, a determination or a review referred to in section 60 (1), or

(d) in an application for judicial review of a decision made under this Act.

(2.3) Subsections (2.1) and (2.2) apply also in respect of evidence of the existence of proceedings conducted before the commissioner.

(3) In conducting an investigation, audit or inquiry under this Act and in a report under this Act, the commissioner and anyone acting for or under the direction of the commissioner must take every reasonable precaution to avoid disclosing and must not disclose

(a) any information the head of a public body would be required or authorized to refuse to disclose if it were contained in a record requested under section 5, or

(b) whether information exists, if the head of a public body in refusing to provide access does not indicate whether the information exists.

(4) The commissioner may disclose to the Attorney General information relating to the commission of an offence against an enactment of British Columbia or Canada if the commissioner considers there is evidence of an offence.

(5) The commissioner may disclose, or may authorize anyone acting for or under the direction of the commissioner to disclose, information in the course of a prosecution, application or appeal referred to in section 45.

Protection of commissioner and staff

48 No proceedings lie against the commissioner, or against a person acting on behalf of or under the direction of the commissioner, for anything done, reported or said in good faith in the exercise or performance or the intended exercise or performance of a duty, power or function under this Part or Part 5.

Saskatchewan – *Freedom of Information and Protection of Privacy Act*, SS 1991 c. F 22.01

Confidentiality
46(1) The commissioner shall not disclose 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) Notwithstanding subsection (1), the commissioner may disclose:
(a) in the course of a review pursuant to section 49, any matter that the commissioner considers necessary to disclose to facilitate the review; and
(b) in a report prepared pursuant to this Act, any matter that the commissioner considers necessary to disclose to establish grounds for the findings and recommendations in the report.

Alberta – *Health Information Act* R.S.A. 2000, c. H-5

Restrictions on disclosure of information by Commissioner and staff
91(1) The Commissioner and anyone acting for or under the direction of the Commissioner must not disclose any information obtained in performing their duties, powers and functions under this Act, except as provided in subsections (2) to (5) and section 50.1.
(2) The Commissioner may disclose, or may authorize anyone acting for or under the direction of the Commissioner to disclose, information that is necessary
(a) to conduct an investigation or inquiry under this Act, or
(b) to establish the grounds for findings and recommendations contained in a report under this Act.
(3) In conducting an investigation or inquiry under this Act and in a report under this Act, the Commissioner and anyone acting for or under the direction of the Commissioner must take every reasonable precaution to avoid disclosing and must not disclose
(a) any health information a custodian would be required or authorized to refuse to disclose if it were contained in a record requested under section 8(1), or
(b) whether health information exists, if a custodian in refusing to grant access does not indicate whether the information exists.
(3.1) The Commissioner may disclose any information to the Minister if in the opinion of the Commissioner the disclosure is necessary to enable the Minister to exercise the powers or carry out the duties or functions of the Minister in respect of any matter under the Minister's administration.
(3.2) The Commissioner may disclose any information to any person where the Commissioner reasonably believes the disclosure of the information to that person
(a) is necessary to protect the privacy, health or safety of an individual, or
(b) is in the public interest.
(4) The Commissioner may disclose to the Minister of Justice and Solicitor General information relating to the commission of an offence under an enactment of Alberta or Canada if the Commissioner considers there is evidence of an offence.
(5) The Commissioner may disclose, or may authorize anyone acting for or under the direction of the Commissioner to disclose, information in the course of a prosecution, application or appeal referred to in section 89(1).

Immunity from suit
92 No action lies and no proceeding may be brought against the Commissioner, or against a person acting for or under the direction of the Commissioner, for anything done, reported

or said in good faith in the exercise or performance or the intended exercise or performance of a duty, power or function under this Part. 1999 cH-4.8

E. ii Order Making versus Recommendation Making Power

Newfoundland – *Access to Information and Protection of Privacy Act Access to Information and Protection of Privacy Act* , 2015 SNL 2015, Chapter A-1.2

Head of public body seeks declaration in court

79. (1) Where the head of the public body decides under section 78 not to comply with a recommendation of the commissioner under subsection 76 (1) in whole or in part, the head shall, not later than 10 business days after receipt of that recommendation,

(a) apply to the Trial Division for a declaration that the public body is not required to comply with that recommendation because the collection, use or disclosure of the personal information is not in contravention of this Act, and

(b) serve a copy of the application for a declaration on the commissioner, the minister responsible for the administration of this Act, and a person who was sent a copy of the commissioner's report.

(2) The commissioner or the minister responsible for this Act may intervene in an application for a declaration by filing a notice to that effect with the Trial Division.

E. iii a Power to Determine Own Procedure

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

45 (2) The commissioner may:

(d) determine the procedure to be followed in the exercise of the powers or performance of any duties of the commissioner pursuant to this Act

E. iii b Power to Compel Production of Records

British Columbia – *Freedom of Information and Protection of Privacy Act* RSBC c. 165

44 (1) For the purposes of conducting an investigation or an audit under section 42 or an inquiry under section 56, the commissioner may make an order requiring a person to do either or both of the following:

(a) attend, in person or by electronic means, before the commissioner to answer questions on oath or affirmation, or in any other manner;

(b) produce for the commissioner a record in the custody or under the control of the person, including a record containing personal information.

(2) The commissioner may apply to the Supreme Court for an order

(a) directing a person to comply with an order made under subsection (1), or

(b) directing any directors and officers of a person to cause the person to comply with an order made under subsection (1).

(2.1) If a person discloses a record that is subject to solicitor client privilege to the commissioner at the request of the commissioner, or under subsection (1), the solicitor client privilege of the record is not affected by the disclosure.
(3) Despite any other enactment or any privilege of the law of evidence, a public body must produce to the commissioner within 10 days any record or a copy of any record required under subsection (1).
(3.1) The commissioner may require a person to attempt to resolve the person's request for review or complaint against a public body in the way directed by the commissioner before the commissioner begins or continues an investigation under section 42 or an inquiry under section 56.
(3.2) Subsection (3.1) applies whether or not a mediator has been authorized under section 55.
(4) If a public body is required to produce a record under subsection (1) and it is not practicable to make a copy of the record, the head of that public body may require the commissioner to examine the original at its site.
(5) After completing a review or investigating a complaint, the commissioner must return any record or any copy of any record produced by the public body concerned.

E. iii c Information Sharing with Other Commissioners

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

45(1) In this section, 'extraprovincial, territorial or federal commissioner' means a person who, with respect to Canada or with respect to another province or territory of Canada, has duties, powers and functions similar to those of the commissioner.
(2) the commissioner may;
(e) exchange personal information with an extraprovincial, territorial or federal commissioner fore the purpose of carrying out investigations with respect to personal information in the possession or under the control of government institutions or to conduct a review involving a government institution and at least one other jurisdiction.

British Columbia – *Personal Information Protection* Act, SBC 2003, c. 63

Restrictions on disclosure of information by commissioner and staff
41 (1) The commissioner and anyone acting for or under the direction of the commissioner must not disclose any information obtained in performing their duties or exercising their powers and functions under this Act, except as provided in subsections (2) to (6).

(6) The commissioner may disclose, or may authorize anyone acting for or under the direction of the commissioner to disclose, information in accordance with an information-sharing agreement entered into under section 36 (1) (l).

General powers of commissioner
36 (1) In addition to the commissioner's powers and duties under Part 11 with respect to reviews, the commissioner is responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may do any of the following:

(k) exchange information with any person who, under legislation of another province or of Canada, has powers and duties similar to those of the commissioner;
(l) enter into information-sharing agreements for the purposes of paragraph (k) and into other agreements with the persons referred to in that paragraph for the purpose of coordinating their activities and providing for mechanisms for handling complaints.

Alberta – *Health Information Act***,** R.S.A. 2000 c. H-5

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. RSA 2000 cH-5 s84;2009 c25

E. iii d Grounds to Refuse to Conduct or Continue a Review

Nova Scotia – *Personal Health Information Act*

95(1) The Review Officer may decide not to review the subject-matter of the review pursuant to clause 92(2)(a) or (3)(a) for whatever reason the Review Officer reasonably considers appropriate, including if satisfied that
a) The custodian has responded adequately to the concerns;
b) The concerns have been or could be more appropriately dealt with, initially or completely, by means of a procedure other than a request for review under this Act;
c) The length of time that has elapsed between the date when the subject-matter of the review arose and the date the review was requested is such that a review under this Section would likely result in undue prejudice to any person;
d) The personal requesting a review does not have a sufficient personal interest in the subject-matter of the review;
e) The request for review is frivolous or vexatious; or
f) The request for review is part of a pattern of conduct that amounts to an abuse of the right of review.
(2) Where the Review Officer decides not to conduct a review under subsection (1), the Review Officer shall give written notice to the custodian and any other person the Review Officer considers appropriate.

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

Review or refusal to review
50(1) Where the commissioner is satisfied that there are reasonable grounds to review any matter set out in an application pursuant to section 49, the commissioner shall review the matter.
(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; or
(c) concerns a trivial matter.

Amendments in Bill No. 30
Section 50 amended
20 The following clauses are added after clause 50(2)(a):
"(a.1) does not affect the applicant or individual personally;
"(a.2) has not moved forward as the applicant or individual has failed to respond to the requests of the commissioner;
"(a.3) concerns a government institution that has an internal review process that has not been used;
"(a.4) concerns a professional who is governed by a professional body that regulates its members pursuant to an Act, and a complaints procedure available through the professional body has not been used;
"(a.5) may be considered pursuant to another Act that provides a review or other mechanism to challenge a government institution's decision with respect to the collection, amendment, use or disclosure of personal information and that review or mechanism has not been used;
"(a.6) does not contain sufficient evidence;
"(a.7) has already been the subject of a report pursuant to section 55 by the commissioner".

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act, 2015*, SNL 2015 c A-1.2

45(1) The commissioner may, at any stage of an investigation, refuse to investigate a complaint where he or she is satisfied that
a) The head of a public body has responded adequately to a complaint;
b) The complaint has been or could be more appropriately dealt with by a procedure or proceeding other than a complaint under this Act;
c) The length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was filed is such that an investigation under this Part would be likely to result in undue prejudice to a person or that a report would not serve a useful purpose; or
d) The complaint is trivial, frivolous, vexatious or is made in bad faith.

(2) Where the commissioner refuses to investigate a complaint, he or she shall
a) give notice of that refusal, together with reasons to the person who made the complaint;
b) advise the person of the right to appeal to the Trial Division under subsection 52(3) or 53(3) the decision of the head of the public body that relates to the request; and
c) advise the person of the applicable time limit and how to pursue an appeal.

E. iii e Time Limits on Commissioner's Processes

British Columbia – *Freedom of Information and Protection of Privacy Act*, RSBC c. 165

The BC law requires that an inquiry must be completed within 90 days after receipt of the appeal (s. 56). However, in practice the British Columbia commissioner reports that it is not always possible to meet this deadline.[100]

British Columbia – *Personal Information Protection Act*, SBC 2003, c. 63, s. 50(8)[101]

50 (8) An inquiry respecting a review must be completed within 90 days of the day on which the request is delivered under section 47 (1), unless the commissioner

(a) specifies a later date, and

(b) notifies

(i) the individual who made the request,

(ii) the organization concerned, and

(iii) any person given a copy of the request

of the date specified under paragraph (a).

Newfoundland and Labrador– *Access to Information and Protection of Privacy Act, 2015*, SNL 2015 c A-1.2

46(1) The commissioner shall complete a formal investigation and make a report under section 48 within 65 business days of receiving the complaint, whether or not the time for the information resolution process has been extended.

(2) the commissioner may, in extraordinary circumstances, apply to a judge of the Trial Division for an order to extend the period of time under subjection (1).

E. iv General Powers of the Commissioner

British Columbia – *Freedom of Information and Protection of Privacy Act,* RSBC c. 165

General powers of commissioner

42 (1) In addition to the commissioner's powers and duties under Part 5 with respect to reviews, the commissioner is generally responsible for monitoring how this Act is administered to ensure that its purposes are achieved, and may

(a) conduct investigations and audits to ensure compliance with any provision of this Act or the regulations,

(b) make an order described in section 58 (3), whether the order results from an investigation or audit under paragraph (a) or an inquiry under section 56,

(c) inform the public about this Act,

(d) receive comments from the public about the administration of this Act,

(e) engage in or commission research into anything affecting the achievement of the purposes of this Act,

(f) comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs or activities of public bodies,

[100] *OIPC Submission to the Special Committee to Review FIPPA* – November 2015 at pp. 44-45.

[101] *Personal Information Protection Act*, SBC 2003, c. 63, s. 50(8).

(g) comment on the implications for access to information or for protection of privacy of automated systems for collection, storage, analysis or transfer of information,

(h) comment on the implications for protection of privacy of using or disclosing personal information for data linking,

(i) authorize the collection of personal information from sources other than the individual the information is about, and

(j) bring to the attention of the head of a public body any failure to meet the prescribed standards for fulfilling the duty to assist applicants.

(2) Without limiting subsection (1), the commissioner may investigate and attempt to resolve complaints that

(a) a duty imposed under this Act has not been performed,

(b) an extension of time for responding to a request is not in accordance with section 10 (1),

(c) a fee required under this Act is inappropriate,

(d) a correction of personal information requested under section 29 (1) has been refused without justification, and

(e) personal information has been collected, used or disclosed in contravention of Part 3 by

(i) a public body or an employee, officer or director of a public body, or

(ii) an employee or associate of a service provider.

Saskatchewan – Bill 30, *Freedom of Information and Protection of Privacy Amendment Act, 2016*

16 Section 45 is repealed and the following substituted:

General powers of commissioner

45(2) The commissioner may:

a) Engage in or commission research into matters affecting the carrying out of the purposes of this Act;

b) Conduct public education programs and provide information concerning this Act and the commissioner's role and activities;

c) Receive representations concerning the operation of this Act;

G. Review of the Acts

Alberta – *Personal Information Protection Act*, S. A. 2003 c. P-6.5

Review of Act

63(1) A special committee of the Legislative Assembly must begin a comprehensive review of this Act and the regulations made under it

(a) by July 1, 2015, and

(b) thereafter, every 6 years after the date on which the previous special committee submits its final report under subsection (2).

(2) A special committee must submit a final report to the Legislative Assembly within 18 months after beginning a review under subsection (1).

(3) The report of a special committee may include the special committee's recommendations for amendments to this Act, the regulations made under this Act or any other enactment.

British Columbia – *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996 c. 165

Review of Act

80 (1) At least once every 6 years, a special committee of the Legislative Assembly must begin a comprehensive review of this Act and must submit a report respecting this Act to the Legislative Assembly within one year after the date of the appointment of the special committee.

(2) A report submitted under subsection (1) may include any recommended amendments to this Act or any other Act.

(3) For the purposes of subsection (1), the first 6 year period begins on October 4, 1997.

Newfoundland and Labrador – *Access to Information and Protection of Privacy Act*, 2015 SNL 2015, Chapter A-1.2

Review

117. (1) 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.

(2) The committee shall review the list of provisions in Schedule A to determine the necessity for their continued inclusion in Schedule A.

Appendix 2:
Bibliography of Recent Reviews of Access and Privacy Laws in Canada

Alberta
Alberta Information and Privacy Commissioner, *Review of the Personal Information Protection Act: Submission to the Standing Committee on Alberta's Economic Future*, February 2016

Alberta Information and Privacy Commissioner, *Producing Records to the Commissioner: Restoring Independent and Effective Oversight under the FOIP Act,* April 2017

British Columbia
British Columbia Information and Privacy Commissioner, *Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, November 2015

Legislative Assembly of British Columbia, *Report of the Special Committee to Review the Freedom of Information and Protection of Privacy Act*, May 2016

Canada
Information Commissioner of Canada, *Striking the Right Balance for Transparency: Recommendations to modernize the Access to Information Act*, March 2015

Privacy Commissioner of Canada, *Privacy Act Reform in an Era of Change and Transparency*, March 23, 2016

House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Review of the Access to Information Act*, June 2016

Newfoundland and Labrador
Wells, Clyde, Doug Letto, and Jennifer Stoddart, *Access to Information and Protection of Privacy Act: Newfoundland and Labrador*, Volume 1: Executive Summary, Volume 2: Full Report, March 2015

New Brunswick
Dr. Ed Doherty, Minister of Government Services, *Review of the Right to Information and Protection of Privacy Act,* August 2015.

Northwest Territories
Government of Northwest Territories, *What We Heard: Results of the Public and Stakeholder Engagement on the Comprehensive Review of the Access to Information and Protection of Privacy Act,* November 2016

Ontario
Information and Privacy Commissioner of Ontario, *Comments of the Information and Privacy Commissioner of Ontario on the Proposed Open Meeting Amendments in Bill 68,* April 2017

Quebec
Commission d'access a l'information du Quebec, *List of Recommendations in the Five-Year Report for 2016*

Saskatchewan
Saskatchewan Information and Privacy Commissioner, *2014-2015 Annual Report: It's Time to Update*

Yukon
Yukon Information and Privacy Commissioner, *Access to Information and Protection of Privacy Act 2015 Review: Information and Privacy Commissioner's Comments*

Yukon Highways and Public Works, *Access to Information and Protection of Privacy (ATIPP) Act Review Report* (December 2016)

This document was prepared by the Office of the Information and Privacy Commissioner for Nova Scotia. We can be reached at:

PO Box 181 Halifax NS B3J 2M4
5670 Spring Garden Road, Suite 509, Halifax
Telephone 902-424-4684
Toll-free 1-866-243-1564
TDD/TTY 1-800-855-0511
www.foipop.ns.ca
Twitter: @NSInfoPrivacy