Government of Newfoundland and Labrador
Submission to the ATIPPA, 2015 Statutory Review Committee

2025 Statutory Review
November 2026

Newfoundland & Labrador

Table of Contents

Introduction **4**
Executive Summary **5**
Part 1 – Review of 2020 Recommendations **10**
1.1 The ATIPP Coordinator 10
1.2 The applicant 11
1.3 The request process 12
1.4 Transfer of requests 14
1.5 Advisory response 14
1.6 Disregarding a request 14
1.7 Vexatious applicants 17
1.8 Timelines and Extensions 17
1.9 Information management and information technology issues 17
1.10 Exceptions to access 19
1.11 Public interest override 28
1.12 Sunset clauses 29
1.13 Veterinary Medical Association 29
1.14 Submissions of the Office of the Speaker of the House of Assembly 29
1.15 Submissions of the Statutory Offices of the House of Assembly 31
1.16 Office of the Information and Privacy Commissioner 32
1.17 Municipalities 34
1.18 Recommendations 4 and 16 of the Muskrat Falls Inquiry 36
1.19 Publication schemes, information directories and proactive disclosure 37
1.20 Protection of privacy 41
1.21 Alumni engagement 51
1.22 Complaints, recommendations and appeals 52
1.23 Other issues 56
Part 2 – Access to Information Provisions **68**
2.1 Designation and delegation by head of a public body 68
2.2 Disregard where behaviour of applicant is abusive or malicious 68
2.3 Managing records provided to the Commissioner by a public body 70
2.4 Section 12 – applicant anonymity 71
2.5 Non-responsive information 72
2.6 Definition of records and exclusion of back-up systems 73

2.7 Jurisdiction of the OIPC related to specific s.5 records 73
2.8 Public prosecution files 74
Part 3 – Privacy Safeguards and Emerging Technologies 80
3.1 Privacy notice content 80
3.2 Making the Act flexible as technology evolves 81
3.3 Proportionality in privacy assessments 82
3.4 Notifying the OIPC of privacy assessments 83
3.5 Inferred personal information 84
Part 4 – Personal Information Protection 86
4.1 Define "sensitive personal information" 86
4.2 Sharing of personal information for connected or integrated service delivery 87
4.3 Data residency 89
4.4 Clarity on minimizing collection 90
4.5 Defining program or service for the purpose of PIA requirements 91
4.6 Privacy assessment requirement and triggers 92
4.7 Privacy of public body employees 92
Part 5 – Privacy Breach Management 95
5.1 Definition of privacy breach 95
5.2 Privacy breach notification 95
Part 6 – Public Body Practices and Accountability 97
6.1 Designate privacy officer 97
Part 7 – Public and Public Body Experience 99
7.1 Cross-reference summary 99
7.2 Government access and privacy professionals' feedback 99
Part 8 – Schedule A Review 101
8.1 Sections of legislation listed in Schedule A 101
8.2 The role of Schedule A around privacy 102
Part 9 – Municipalities 103
9.1 Municipal issues cross-reference 103
Conclusion 104

Introduction

The Minister responsible for the administration of the **Access to Information and Protection of Privacy Act, 2015** ("the **Act"**) is required under section 117 of the **Act** to refer the **Act** to a committee for comprehensive review every five years. The ATIPP Office assists with this mandate by providing guidance and assistance to public bodies that are subject to the **Act**. This includes developing and issuing policies, procedures, and guidance materials; designing and delivering training; and operating a support line for public bodies seeking guidance or assistance.

This submission is prepared by the ATIPP Office on behalf of the Government of Newfoundland and Labrador, in collaboration with the various departments within government.

This submission responds to the 2025 review, which is being conducted by Keri-Lynn Power.

It is the government's view that the suggestions in this submission will improve both the access and privacy provisions of the **Act**, while upholding its primary purposes: ensuring transparency, accountability, and public participation, and protecting the privacy of individuals in relation to personal information held by public bodies.

This submission is structured to align with the Terms of Reference for the Statutory Review Committee for ease of reference. Generally, the positions put forward by government in the 2020 statutory review are still relevant, unless otherwise noted in relation to the specific items discussed through this submission.

Executive Summary

Newfoundland and Labrador has a strong foundation for advancing an access and privacy regime that continues to support transparency, accountability and public participation while safeguarding the personal information entrusted to public bodies. As public services become more digital, interconnected and data-driven, there is an opportunity to modernize the framework so it remains responsive, resilient and effective. New technologies, evolving information practices and growing service expectations create opportunities to strengthen how information is managed, accessed and protected. This submission identifies key priorities for building a modern and balanced regime that supports innovation, reinforces public trust and equips public bodies of all sizes to meet the needs of the future.

Building on this foundation, government's approach is focused on forward-looking, practical improvements that balance transparency, privacy protection and effective public administration. While the submission addresses a broad range of considerations, its most substantive proposals are organized around three key themes: strengthening timely and efficient access to information; enhancing privacy protections; and modernizing the legislative framework for an evolving privacy and technology landscape.

Theme 1: Strengthening timely and efficient access to information

The submission identifies several practical measures that would have the greatest impact on the timeliness and efficiency of the access process.

- **Proactive disclosure** and practical **publication schemes** offer opportunities to enhance both transparency and efficiency. Publishing commonly requested information can make useful records available more quickly and reduce reliance on the formal access request process. Establishing publication schemes that are practical and reflect the various resources and capacities of public bodies would deliver meaningful value to the public while supporting sustainable implementation by public bodies (detailed at Section 1.19 – Orsborn recommendations 74-76).

- The submission identifies opportunities to **streamline administrative steps** and direct coordinator time toward activities that add the greatest value for applicants: clarifying requests, locating records, consulting where necessary, reviewing responsive information and preparing final responses.

  The advisory response requirement has created additional steps and effort by public bodies and includes information similar to what is provided in the initial acknowledgement letter. Any updates on the file should be communicated by coordinators throughout the request process, as appropriate. Removing the legislative requirement to issue an **advisory response** would help streamline current processes by

removing unnecessary and redundant administrative efforts (detailed at Section 1.5 – Orsborn recommendation 15).

Practical timeline adjustments would further enable timely access. Specifically, allowing **short extensions** to be issued by the public body with notice to the Officer of the Information and Privacy Commissioner (OIPC) would give public bodies the ability to extend a request timeline, under specific circumstances, by no more than 10 business days without needing to apply to the OIPC. This would improve public bodies' ability to process requests and remove the administrative efforts currently required to seek a short extension (detailed at Section 1.8 – Orsborn recommendation 24). Additionally, allowing public bodies to extend the time limit where the applicant and public body agree to the extension would also allow for a more efficient process (detailed at Section 1.8 – Orsborn recommendation 25).

Adjusting timelines set out in the Act to allow for more reasonable timelines in specific circumstances would provide public bodies sufficient time to make informed decisions while supporting timely access to information for applicants. Extending the **time to transfer a request** from five business days to 10 would give public bodies additional time to determine if a transfer is necessary and which public body may have the records being requested (detailed at Section 1.4 – Orsborn recommendation 13). Adjusting the **time for filing an application with the OIPC to disregard** a request would respond to the practical issues experienced by public bodies when assessing whether to seek approval to disregard. There is a significant amount of work that is required for a public body to make an informed decision about whether to seek a disregard, including clarifying the request with an applicant, initial records search, and discussion with subject matter experts. Once a decision is made to request a disregard, the public body must prepare a formal request which takes time to ensure adequate details and evidence are provided for the OIPC to make their decision whether to grant the application to disregard. Extending the time from five business days to 10 would allow for more time to work with applicants or to complete the work required to make such an application (detailed at Section 1.6 – Orsborn recommendation 17).

- General access requests should continue to remain largely free with **no application fees**, with processing fees being applied only after significant free time, helping public bodies manage unusually resource-intensive requests while continuing to provide timely access to all applicants. Government supports the 2020 review recommendation to permit processing fees only after a substantial amount of free processing time. This is intended to help ensure that unusually large or complex requests can be managed without affecting timely service for other applicants. Personal information requests would remain free.
- The current **definition of "business day"** under ATIPPA, 2015 does not reflect actual business days for public bodies. A number of holidays observed by public bodies are considered "business days" as defined in the Act. Updating the definition of "business

day" as suggested in the 2020 review would more accurately reflect the days that public bodies are open (detailed at Section 1.23(iii) – Orsborn recommendation 115).

- Government's submission proposes **updating certain exceptions to disclosure** and **clarifying procedural processes relating to OIPC complaints.** By removing "supplied in confidence" from to third party business information, the aim can be on the primary purpose of the exception which focuses on harm (detailed at Section 1.10(ix) – Orsborn recommendation 47). By updating workplace investigations, the Act can better reflect its two purposes – openness and transparency – through the disclosure of the final report to affected parties, while ensuring the safety and privacy of others is properly protected. This will further protect internal workplace investigation processes which are essential to a safe and healthy workplace (detailed at Section 1.10(vi) – Orsborn recommendations 40-44).

- Furthermore, it is important to ensure that other legal processes essential to the functioning of society are not overlooked or ignored – these must be considered as it relates to ATIPPA, 2015 and incorporated to properly support the purposes of the Act – particularly as it relates to settlement privilege (detailed in Section 1.10(iv) – Orsborn recommendation 38) and prosecution files (detailed in Section 2.8). The submission also proposes clarifying OIPC procedures for records that fall outside the scope of the Act or are protected by solicitor-client privilege. Formalizing these existing practices would provide greater certainty (detailed at Section 1.10(iii) – Orsborn recommendations 36–37 and suggestion 1, and Section 2.7, respectively).

Theme 2: Enhancing privacy protections

The privacy landscape continues to evolve rapidly as digital services, data practices and public expectations have become increasingly complex. Having a strong governance framework and clear enhanced privacy obligations would strengthen privacy protections for personal information and reflect the current landscape.

- **Designating a privacy officer** within a public body would support privacy accountability within the public body. This role would serve as a touchstone for privacy matters, including privacy training, advising on privacy assessments, responding to privacy breaches, and developing privacy policies. Having a clear requirement for a privacy officer demonstrates the importance of ensuring personal information is safeguarded by the public bodies that hold it. Recognizing that public bodies will have varying privacy risks and differing resources, having an adaptive approach to privacy officer functions and roles should be considered (detailed at Section 6.1).

- **Privacy assessments** present another opportunity to strengthen privacy protections in program design. Incorporating necessity and proportionality into privacy assessments would help public bodies focus resources most effectively and ensure privacy impacts are appropriately assessed. With this change, public bodies would consider whether a proposed collection, use or disclosure advances a legitimate purpose, whether the

approach is proportionate to the expected benefit and whether a less privacy-intrusive option could achieve the same result. This would tailor the depth of assessment to the sensitivity and volume of information, the purposes for which it is used, and the nature of the program or technology (detailed at Section 3.3).

- Establishing a risk-based approach to **engagement with the OIPC on privacy assessments** would provide enhanced oversight of privacy risks and mitigations for programs or services. Currently, public bodies are required to notify the OIPC of a privacy assessment only where it relates to a common or integrated program or service. This approach does not contemplate engagement with the OIPC where a program or service might pose a high risk. Establishing a risk-based approach for OIPC engagement on privacy assessments would require public bodies to consult on initiatives involving significant privacy considerations. This model would strengthen oversight for higher-risk initiatives while allowing routine, lower-risk projects to proceed efficiently (detailed at Section 3.4).

- Enabling **connected and integrated service delivery** is another important element that highlights the need to modernize legislation to reflect the increasing expectation for integrated, seamless services. Integrated services can reduce the need for individuals to provide the same information repeatedly and make interactions with government simpler and more efficient. Establishing a clear legislative framework helps enable development of connected or integrated service, including the ability to designate an identity information service provider to support these services. Clearly defined authority, supported by strong privacy safeguards, would provide public bodies with greater certainty when designing integrated services. It would also strengthen public trust by ensuring that personal information is shared within a clear and accountable privacy framework (detailed at Section 4.2).

Theme 3: Modernizing the legislative framework for an evolving privacy and technology landscape

Technology, service delivery and privacy practices continue to evolve rapidly, creating an opportunity to design a framework that can adapt over time. The Act should continue to establish core rights, duties and principles, and overall privacy obligations, while regulations and policy provide the detailed and adaptable requirements needed to support these obligations.

- A **regulation-based approach** is particularly important for privacy obligations affected by technological change. Government's submission identifies areas where regulation-making authority could help maintain flexibility, including reasonable security standards, privacy assessment content, algorithmic impact assessment content, automated decision making definitions, information-sharing agreements, privacy notices, data residency, breach-risk definitions and safeguards for connected services. This approach would allow the framework to remain current and adaptable as technologies, risks and

privacy practices evolve, without requiring frequent statutory amendment (detailed at Section 3.2).

- **Data residency** highlights another area for strengthening the protection of digital information. The submission suggests a Canadian storage requirement, with regulations authorizing appropriate circumstances for disclosure, storage or access outside Canada. This approach would establish a clear legislative foundation for assessing foreign legal regimes, vendor structures, cross-border access and data ownership, while retaining flexibility to support secure and effective service delivery (detailed at Section 4.3).

- New and rapidly changing technologies are being used more frequently. Clearly defining terms describing certain kinds of technologies will help to provide clarity on the systems being used that may impact privacy as well as the processes used to assess risks. The submission supports **clear definitions of automated decision systems and algorithmic impact assessments**, with obligations focused on systems that make or materially assist decisions about identifiable individuals using personal information, particularly where the effects are legally or otherwise significant. Distinguishing these systems from routine routing of information, formatting documents, or other administrative functions would support responsible innovation while concentrating safeguards on uses with the greatest impact on individuals (detailed at Section 1.20(iv) – Orsborn recommendations 86 a and b).

  Government's artificial intelligence (AI) policy identifies transparency and explainability as one of its guiding principles for the responsible use of AI. This principle aligns with the foundational privacy principle of openness. Requiring public bodies to notify individuals when an automated decision system is used to make or materially assist a decision about them would reinforce this alignment and embed a clear transparency requirement in law (detailed at Section 3.1).

  Additionally, establishing a standalone IT security exception to disclosure is reflective of the new technological realities in which public bodies work (detailed in Section 1.10(xi) - Orsborn recommendation 53).

Together, these suggested changes offer a practical and balanced path to modernizing the Act, strengthening access and privacy protections, and ensuring the framework remains responsive to evolving public needs and technological change.

Part 1 – Review of 2020 Recommendations

Terms of Reference, Mandate Area 1: consideration of the 2020 Statutory Review recommendations issued by the Honourable David B. Orsborn, for applicability or revision.

1.1 The ATIPP Coordinator

#	2020 Recommendation (summary)	Notes
1.	That the head of each public body provide each designated ATIPP coordinator with a formal mandate letter.	No longer required for government. See commentary below.
2.	That the Classification and Organization Division section of Treasury Board develop a job description and classification for the position of full-time coordinator.	No longer required for government. See commentary below.
3.	That each coordinator sign an oath/affirmation of confidentiality addressing their particular obligations as coordinators.	Government is supportive of this recommendation.

Recommendation 1 (mandate letter)
The implementation of the new ATIPP Office structure in December 2024 resulted in the creation of consistent position descriptions for access to information ("ATI") coordinators and senior ATI coordinators. These position descriptions clearly set out the role and function of these positions within government. In addition, the ATIPP Office revised the formal delegation of authority form for departments to also clearly outline the authorities that are delegated to the Senior ATI coordinator and ATI coordinator for each department. As such, providing coordinators with a mandate letter is no longer required for government.

Government is supportive of public bodies providing their coordinator with a formal mandate letter. The ATIPP Office is available to assist in preparing a standard letter for public body use.

Recommendation 2 (position description)
There are now consistent position descriptions within government for all ATI and senior ATI coordinators. During the creation of consistent position descriptions, these positions went through the position classification process, resulting in a consistent classification for ATI coordinators and senior ATI coordinators within government. As such, this recommendation is complete and is no longer required.

1.2 The applicant

#	2020 Recommendation (summary)	Notes
4.	Require the full name and contact information of the applicant for all requests.	Government is supportive of this recommendation.
5.	Make it clear that the anonymity of an applicant continues to apply following the final response to the applicant.	Government is supportive of this recommendation.
6.	Provide that within 5 days of receiving a request, public bodies may ask for identity verification (for personal information requests) or clarification of the request, and applicants must respond within 30 days or their request will be considered abandoned.	Government is supportive of this recommendation.
7.	Stop the clock on time limits for final responses while waiting for an applicant's response to a request for clarification or identity verification.	See commentary below.

Recommendation 7 (clock stop)

Issue:
ATI coordinators have advised of instances where contacting an applicant to verify their identity has been challenging and has affected their ability to respond within the legislated timelines, where that information is needed for processing the request. When considering some of the other recommendations put forward by Justice Orsborn that would support coordinators in these circumstances (e.g. recommendations 20 and 24) and the intent of the **Act** (to provide timely access to information), government is of the opinion that this recommendation may not be necessary with the acceptance of recommendations 20 and 24.

If recommendations 20 and 24 are implemented, public bodies would have other mechanisms to manage requests from unidentifiable applicants and to obtain short extensions in appropriate circumstances. A separate clock-stop provision may duplicate those tools.

In addition, stopping the clock could create uncertainty for applicants. Applicants may not know when the timeline has paused, restarted, or how long the overall process may take. This could reduce predictability and confidence in the access process.

Suggestion: No change required to stop the clock should recommendations 20 and 24 be implemented.

1.3 The request process

i) Fees and costs

#	2020 Recommendation (summary)	Notes
8.	That the **Act** be amended to charge the cost of time spent identifying, locating, retrieving, reviewing, severing and redacting records for individual requests in excess of 35 hours, subject to the existing estimate, waiver, review and other provisions of section 26.	Government is supportive of this recommendation.
9.	That the **Act** be amended to allow public bodies to charge fees per page for physical reproduction of records in excess of 100 pages.	Government is supportive of this recommendation with modification. See commentary below.
10.	That the responsible minister revise the current cost schedule to reflect the recommendations in this report.	Government is supportive of this recommendation.

Recommendation 9 (charging for physical reproduction of records)

Issue:
This recommendation supports the continued use of a largely cost-free access regime while recognizing that large paper-based requests can create additional costs for public bodies. A 100-page threshold means that applicants would not be charged for ordinary copying, but a public body could recover some costs where a request requires a significant amount of physical reproduction. This would be most relevant where an applicant asks for paper copies or where records cannot reasonably be provided electronically. The cost schedule should clearly state when these fees apply so applicants know the potential cost before deciding how they want to receive the records.

Consideration should be given to whether local public bodies should be excluded at this time given the significant variation in their size, staffing, and administrative capacity in processing access to information requests.

Suggestion: Implement this change for government departments and other public bodies, except for local public bodies.

---

ii) Record format

#	2020 Recommendation (summary)	Notes
11.	That the **Act** be amended to specify that when a record exists in a format specifically requested, a public body should provide it in that format when it is reasonably practicable. Otherwise, it can be provided in a format either agreed upon with the applicant or that does not materially change the content. (Any record provided, regardless of format, remains subject to redaction in accordance with the exceptions in the **Act**).	See commentary below
12.	That the OCIO and the ATIPP Office make available to the smaller public bodies basic training and information responding to requests for a record in a particular format.	See commentary below

Recommendation 11 (native file format)

Issue:
In 2015, the ability to request information in a usable electronic format was introduced in s. 20 of the **Act**. This was to specify in the **Act** that applicants could receive usable data sets, where possible, instead of receiving only paper copies or unworkable PDFs at the discretion of the public body. This was primarily beneficial to applicants if a responsive record was a data set, such as a spreadsheet and meant that the record could be usable beyond merely providing information. Recommendation 11 would allow applicants to request and receive information in its original form (i.e., native format'), as it exists in and is used in the public body. For example, if an applicant requested emails in native format, they would receive the actual email (e.g. msg file) and not a copy or PDF.

Currently, most records are provided to applicants in "near-native" format, which is described by OCIO as a format which "produces the data contained in the document with as much original information as possible in a different, often more easily accessible file type." To be able to apply redactions, files are required to be converted to specific formats that allow for redactions (e.g. an email is converted to a PDF to be able to apply redactions – this is a redaction software requirement).

Furthermore, there are potential unintended consequences associated with providing records in native format. Metadata in a native format may reveal additional information about the file or its content which may include IT security information (i.e. IP addresses and server names). This could pose a security risk where the metadata includes IT security information.

Suggestion: Maintain section 20 as it is currently written.

Recommendation 12 (training re: native file format)
As this recommendation is directly tied to recommendation 11, training on providing records in native file format would not be required, based on the suggestion above.

1.4 Transfer of requests

#	2020 Recommendation (summary)	Notes
13.	That the **Act** be amended to expand the window for transferring requests between public bodies to 10 days.	Government is supportive of this recommendation.
14.	That concurrently with the transfer of an access request to another public body, the transferring coordinator notify the ATIPP Office of the transfer.	Government is supportive of this recommendation. This is consistent with current practices.

1.5 Advisory response

#	2020 Recommendation (summary)	Notes
15.	That the **Act** be amended to remove the requirement for advisory responses.	Government is supportive of this recommendation.
16.	That acknowledgement letters be automatically generated and sent to applicants when a coordinator confirms receipt of a request.	This is no longer required as this functionality is now included in the new ATIPP Office case management system for government departments.

1.6 Disregarding a request

#	2020 Recommendation (summary)	Notes
17.	Extend the period in which to apply for a disregard to 10 days.	Government is supportive of this recommendation.
18.	Remove the ability to apply to disregard a request on the basis of unreasonable interference with the public body.	See commentary below.
19.	Stop the clock on time limits for final responses while waiting for the commissioner's approval of a disregard application.	See commentary below.

#	2020 Recommendation (summary)	Notes
20.	Allow the head of a public body to approve disregard applications in cases of requests for information otherwise accessible to any applicant and requests from unidentifiable applicants. The commissioner must be notified in writing.	Government is supportive of this recommendation.
21.	That where the head of a public body disregards a request, the coordinator of the public body notify the ATIPP Office of the disregard and reasons therefor.	Government is supportive of this recommendation. This is consistent with current practices.

Recommendation 18 (disregard on basis of unreasonable interference)

Issue:
The 2020 Committee recommended removing the ability to request approval from the commissioner to disregard requests on the basis of unreasonable interference with the public body (s.21(1)(a)). This specific provision was not suggested by any stakeholder during the review and therefore no submissions focused on this particular item.

In order for the commissioner to consider approving a disregard for this purpose, in most instances, a public body must show that they have tried to work with the applicant to make the request more manageable. Therefore, in most instances, it is only where an applicant chooses not to work with a public body that the OIPC will approve such a disregard.

A recent British Columbia OIPC order provides a useful example where timing of a request and the staff who would have the records could result in unreasonable interference with the public body's operations. In **Order F24-07, Provincial Health Services Authority**, the applicant requested statistical information related to COVID-19 and vaccination status. The Provincial Health Services Authority advised that the requested record did not exist and that producing it would require specialized work to combine raw data, generate statistics, and complete analysis and review by staff with public health and data expertise. In this situation, given the records did not exist at the time, the adjudicator confirmed that the duty to assist did not require the public body to create the requested record in those circumstances.

This type of case illustrates why retaining the ability to seek authorization to disregard a request where responding would unreasonably interfere with operations remains important. The issue is not always that a request is frivolous, vexatious, abusive, or excessively broad on its face. In some cases, the request may be legitimate, but responding at that time would require the expertise of a small number of key staff who are needed for urgent operational work, such as public health response, emergency management, or another time-sensitive public service function. Existing disregard grounds may not capture that kind of operational reality.

Several Canadian jurisdictions include a similar provision (British Columbia, Manitoba, Quebec, Yukon).

Having the ability to request to disregard requests in these extraordinary circumstances where the request itself is not unreasonable but the timing and context could have serious impacts on operations is an important element to s.21.

It is important to note that the provisions governing applications for approval to disregard a request are used only in the most extraordinary circumstances and after the coordinator has exhausted all other avenues to respond to the request, including reaching out to the applicant to clearly identify what records they are seeking, trying to establish a timeframe for a search of records, etc. An application to disregard under s.21(1)(a) requires review and consideration by the commissioner, ensuring independent oversight and a decision that is founded only through evidence establishing whether it meets the high threshold required to disregard a request.

It should also be emphasized that the decision to authorize a public body to disregard a request rests with the commissioner, not the public body. A public body may only request authorization and must provide sufficient evidence to demonstrate that the statutory threshold has been met. The commissioner then makes an independent decision based on the relevant facts, evidence, and factors in the circumstances. This independent oversight preserves accountability and ensures that the decision to disregard a request rests with the commissioner.

Suggestion: Retain s.21(1)(a) as it is currently written.

Recommendation 19 (Stop the clock during a disregard application)

Issue:
During the 2020 review of the **Act**, public bodies brought forward recommendations regarding "stopping the clock" as it relates to various procedures. This included when waiting for the OIPC to respond to an application for approval to disregard a request. Under subsection 21(2), the OIPC has three business days to respond to such a request. It was argued that in the event that the OIPC does not approve the application that this would essentially result in the public body losing 3 of the 20 business days they have to respond to a request (given the nature of a disregard application in most instances a public body would not be able to continue to work on the request while waiting for a response).

While government understands the concern that time spent waiting for the OIPC's decision could affect the public body's ability to meet the 20-business-day response timeline, this must be balanced against the **Act's** objective of providing timely access to information. When considered together with recommendation 24, which would allow public bodies to extend the response timeline by up to 10 days in specified circumstances, a separate clock-stop provision for an application to disregard a request is not required.

Suggestion: No change is required to stop the clock during a disregard application if recommendation 24 is implemented.

1.7 Vexatious applicants

#	2020 Recommendation (summary)	Notes
22.	Allow the head of a public body to ask the commissioner to declare an applicant to be a vexatious applicant for a period of time determined by the commissioner.	Government is supportive of this recommendation.
23.	Allow an applicant to appeal a vexatious applicant declaration to the court and allow the court to make an appropriate order.	Government is supportive of this recommendation.

1.8 Timelines and Extensions

#	2020 Recommendation (summary)	Notes
24.	Allow the head of a public body to approve, in specified circumstances, an extension to the time limit for a response of up to 10 days based on a written recommendation from the coordinator. The commissioner must be notified in writing.	Government is supportive of this recommendation.
25.	Allow the head of a public body and an applicant to agree to an extension to the time limit for a response. The commissioner must be notified in writing.	Government is supportive of this recommendation.
26.	That where the head of a public body approves an extension, the coordinator notify the ATIPP Office of the reasons for and length of the extension.	Government is supportive of this recommendation. This is consistent with current practices.

1.9 Information management and information technology issues

#	2020 Recommendation (summary)	Notes
27.	That OCIO and the ATIPP Office conduct a review of the HP Records Manager and Online Tracking System with a view to system integration and/or a meaningful reduction of effort arising from the duplication of systems.	This recommendation is specific to core government departments and offices under Executive Council. This is no longer required with the introduction of the ATIPP Office's new case management system which

#	2020 Recommendation (summary)	Notes
		replaces the disparate systems previously used.
28.	That OCIO, the ATIPP Office and relevant department(s) conduct a review of the Online Request System with a view to making the online system available to such other public bodies who may wish to avail of it.	Government is supportive of this recommendation.
29.	That OCIO and the ATIPP Office investigate and take steps as appropriate to provide coordinators with pre-authorized, continuous access to frequently searched email accounts.	This is no longer required with the move to Microsoft M365. Coordinators now have continuous access to search accounts within their assigned department.
30.	That the Government Records Committee constituted under the **Management of Information Act** review its guidelines and policies with respect to the identification and disposal of transitory emails.	Government is supportive of this recommendation.
31.	That the head of each public body subject to the **Management of Information Act** ensure that their record management system properly reflects the approved guidelines for transitory records and that the identification and appropriate disposal of transitory emails is carried out accordingly.	Government is supportive of this recommendation.
32.	That each public body not subject to **Management of Information Act** review the content of and compliance with any existing guidelines for the disposal of transitory emails or develop guidelines forthwith.	See commentary below.

Recommendation 32 (transitory email guidelines for other public bodies)

Issue:
This recommendation raises broader questions about the appropriate information management framework for public bodies that are outside the scope of the **Management of Information Act (MOIA)**. While consistent guidance on the disposal of transitory emails may be beneficial, further work would be required to determine the appropriate legislative or

policy mechanism, the extent of government's role, and whether a common approach could be applied across different types of public bodies.

Suggestion: Consider developing guidance, in consultation with affected public bodies, to support consistent management of transitory emails outside the **MOIA** framework.

1.10 Exceptions to access

i) Cabinet confidences

#	2020 Recommendation (summary)	Notes
33.	That the **Act** be amended to remove "decisions" from the definition of "Cabinet record".	See commentary below.

Recommendation 33 (definition of Cabinet record)

Issue:
Section 27 (1) of the **Act** defines "cabinet record" and requires public bodies to refuse access to these records. Paragraph 27(1)(e) includes "an agenda, minute or other record of Cabinet recording deliberations or decisions of the Cabinet". The definition of Cabinet record comes directly from the **MOIA**.

Removing the term "decisions" from s.27(1)(e) would not remove minutes of council from the current definition of a Cabinet record, where most decisions are recorded. Furthermore, it would not necessarily remove it from protection under "substance of deliberations." Such "decisions" therefore, would be subject to a line-by-line review versus a redaction at the record level. Accepting this recommendation would not change what can be protected as a cabinet confidence but would add confusion to the process of reviewing records and determining which paragraph or subsection may apply.

Suggestion: No change is required to s.27(1)(e).

---

ii) Local public body confidences

#	2020 Recommendation (summary)	Notes
34.	Make it clear that privileged meetings of a municipal council committee have the same exceptions to disclosure as privileged meetings of the council.	Government is supportive of this recommendation.

#	2020 Recommendation (summary)	Notes
35.	Remove regulation-making authority relating to privileged meetings of a local public body or committee.	Government is supportive of this recommendation.

iii) Solicitor-client privilege

#	2020 Recommendation (summary)	Notes
36.	That the **Act** be amended to make it clear that the OIPC can require the production to it of records over which solicitor-client privilege is claimed when production is determined to be absolutely necessary to assess the claim for privilege, but no production may be ordered when the privilege relates to advice given in respect of an ATIPP matter.	See commentary below.
37.	That the **Act** be amended to provide that the commissioner's right of entry and examination and copying of a record does not extend to a record over which solicitor-client privilege is claimed.	Government is supportive of this recommendation.
	Suggestion 1: Public bodies support claims of solicitor-client privilege with a solicitor's affidavit and a listing and description of each document.	See commentary below.

Recommendation 36 (production of solicitor-client privileged records to the OIPC)

Issue:
Since the 2020 review, there have been court decisions within Newfoundland and Labrador that have determined the OIPC does not have the ability to compel production of solicitor-client privileged records. In Newfoundland and Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Justice and Public Safety), 2023 NLCA 27, the Court of Appeal concluded that "despite evidence of legislative review and recommendations for change to the impugned sections of the **Act** , [they] would agree with the applications judge that the language of the **Act** is not sufficiently clear, explicit and unequivocal to set aside solicitor-client privilege."."

As a result, government departments do not provide solicitor-client privileged records to the OIPC. However, government has implemented a process that balances this fundamental privilege, while also ensuring the OIPC is provided sufficient detail to meet the burden of proof contemplated by s.43. In OIPC report A-2024-004 the Commissioner found that the "provided chart contains brief descriptions of the records redacted and the pages withheld,

page numbers, record type, and names of both recipients and senders [and]…is sufficient to discharge the Department's burden under section 43."

In considering whether to recommend amendments to the **Act** to explicitly state that the OIPC can compel production of solicitor-client privileged records, as proposed by the 2020 **ATIPPA, 2015** Review Committee, it is essential that the purpose of this privilege and its importance as a principle of fundamental justice is considered. In the Court of Appeal decision referenced above, the Court found:

> The question before this Court is the same as it was in *Calgary*, namely, does the Commissioner have the right to compel production of solicitor-client records. I would conclude therefore that the facts of this case also engage solicitor-client privilege in its substantive context and that as a substantive rule, solicitor-client privilege must remain as close to absolute as possible and should not be interfered with unless absolutely necessary.

It is this government's position that the language in the **Act** should not be modified to allow this fundamental privilege to be reviewed by the OIPC. It would further question under what circumstances production would be "absolutely necessary"? The current practice is to provide the OIPC with a list describing records withheld under section 30. The OIPC has found that this practice meets the burden under section 43. Additionally, there are mechanisms that currently exist with the **Act** and the court system which would allow the review of these records by the court in instances where it was deemed necessary for the records to be reviewed. This position is supported by the Court of Appeal which further concluded that:

> In closing, I would note as the Court did in *Calgary* at paragraph 59, that the Court's conclusion on the Commissioner's inability to compel production of records subject to solicitor-client privilege does not leave an applicant without recourse when a public body refuses to produce solicitor-client records. In such an instance, an applicant can appeal the refusal directly to the Supreme Court of Newfoundland and Labrador, under section 52 of **ATIPPA 2015** and adjudication of issues associated with the claim of solicitor-client privilege would, as is traditional, be addressed by the courts.

Given the above, and given there are other mechanisms in place to resolve issues concerning solicitor-client privilege (i.e. the Courts), it is government's position that the language of the Act should remain as is.

Suggestion: No change is required to the legislation.

Suggestion 1 (provide a solicitor's affidavit and listing and description of each document)

Issue:
It is government's position that it would not be appropriate for a solicitor to sign an affidavit as it could result in the solicitor being a witness in the event of an appeal.

Current practice for government is to provide the OIPC with a listing and description of each document where solicitor-client privilege has been applied. In OIPC report A-2024-004 the Commissioner found that the "provided chart contains brief descriptions of the records

redacted and the pages withheld, page numbers, record type, and names of both recipients and senders. While not a sworn affidavit, the chart in my view contains more information than contained in the affidavit referenced in A-2023-039 and is sufficient to discharge the Department's burden under section 43."

Suggestion: No change required.

---

iv) Settlement privilege

#	2020 Recommendation (summary)	Notes
38.	That the **Act** be amended to include settlement privilege in subsection 30(2).	Government is supportive of this recommendation with modification. See commentary below.

Recommendation 38 (settlement privilege)

Issue:
Currently there is no provision within the **Act** that protects settlement privilege. While this is a common law privilege, the OIPC has found that it cannot be applied to an access request as it is not within the **Act**, which is a complete code. Without settlement privilege contained within the **Act**, third parties may be reluctant to entertain settlement discussions with a public body if it knows that its confidential settlement discussions could be made public. This is particularly so where admissions would be made and concessions offered that may be detrimental to the third party. However, government recognizes that there are circumstances where some information regarding settlements are in the public interest to disclose.

In their final report - when reviewing whether to include settlement privilege in the **Act**, the 2020 Review Committee determined that s.35(1)(g) of the **Act** was sufficient to protect privilege of a public body. However, they did recommend that third party privilege be protected under s.30(2) of the **Act** – "The head of a public body shall refuse to disclose to an applicant information that is subject to solicitor and client privilege or litigation privilege of a person other than a public body." This is a mandatory exception, meaning that if the information in question fits within the third party's settlement privilege it cannot be released – a public body would have no discretion. The Committee further found:

> "where other than a public body is concerned, the disclosure of information determined to be privileged should not, in the context of **ATIPPA, 2015**, be subject to a further test involving commercial harm or otherwise. The public interest is served by having settlement-privileged information of a public body subject to a discretionary harm-based"

It is unclear how this recommendation will work in practice, as settlement privilege belongs to all parties to the settlement. Unless a public body is settling with another public body the privilege will be shared with a third party. If the privilege belongs to both a public body and a third party, then it would automatically fall under s.30(2), which as noted above, is a mandatory exception to disclosure. This could result in information that the Chair had contemplated to fall within a discretionary exception to fall within the mandatory exception – providing a public

body with no ability to disclose the information even where it may be appropriate or in the public interest to do so.

For these reasons, government is recommending that settlement privilege fall within s.30(1) of the **Act** – this will balance the need to ensure that settlement privileges are appropriately protected, while ensuring that there is discretion to release where appropriate, and making settlement privilege subject to the public interest override (s.9). This option is further supported by similar approaches being implemented in other jurisdictions.

In its amended **Freedom of Information and Protection of Privacy Act** **("FOIPOP")** coming into force in 2027, Nova Scotia defines "legal privilege" under s.3 as including "solicitor-client privilege, litigation privilege and settlement privilege".

While most other jurisdictions do not explicitly refer to settlement privilege, the comparable exceptions to disclosure relating to legal advice are broader and would capture settlement privilege. For example:

- "any type of legal privilege" (PE, MB, AB);
- "a legal privilege" (YK); or
- "any type of legal privilege available at law" (SK, NT, NU).

Suggestion: Modify recommendation to include settlement privilege under s.30(1) rather than s.30(2).

---

v) Confidential evaluations

#	2020 Recommendation (summary)	Notes
39.	That the **Act** be amended to include an exception to disclosure of the confidential assessment of research carried out under the authority of the Health Research Ethics Authority.	Government is supportive of this recommendation.

vi) Workplace investigations

#	2020 Recommendation (summary)	Notes
40.	Extend the definition of "workplace investigation" to include others holding a position within a public body.	Government is supportive of this recommendation.
41.	Provide a mandatory exception to access for all relevant information created or gathered for the purpose of a workplace investigation, but allow discretionary disclosure of the final report of a workplace investigation to a	Government is supportive of this recommendation with modification. See commentary below.

#	2020 Recommendation (summary)	Notes
	complainant or respondent, or otherwise where in the public interest.	
42.	Require the head of a public body to disclose to an applicant a statement provided by the applicant for the purpose of a workplace investigation.	Government is supportive of this recommendation.
43.	Remove the **House of Assembly Act** and **House of Assembly Accountability, Integrity and Administration Act** inquiries from s. 33.	Government is supportive of this recommendation.
44.	Allow the head of a public body to refuse access to information relating to workplace conduct provided in confidence, including opinions about another individual.	Government is supportive of this recommendation.

Recommendation 41 (final report of a workplace investigation)

Issue:
During the 2020 ATIPPA review, it was recognized by most stakeholders that section 33 of the **Act**, as currently worded, is problematic and is having negative impacts on workplace investigations completed by public bodies. As a result of the concerns raised in submissions, public hearings and during a roundtable discussion specifically on s.33, the Chair made several recommendations regarding this section which government supports (see above table).

While government supports the spirit of this recommendation, it is concerned that allowing discretion over whether to release the final report would not meet procedural fairness requirements for people who are a party to a workplace investigation. For this reason, government is suggesting that the "shall" in subsection 33(3) remain for the final report. However, recognizing that a final report could contain highly sensitive personal information that should not be released, or information that could impact someone's safety, it would be necessary to include limited discretionary exceptions to disclosure within this mandatory subsection (i.e. privacy under s.40 and for health and safety reasons under s.37).

As it relates to the recommendation to disclose the report if in the public interest, it is suggested that the public interest override fall within s.33 rather than s.9 of the **Act**. This would be in line with other mandatory exceptions such as section 40 (personal information). This mandatory exception is unique and often the records that fall under it are of a highly sensitive nature. To ensure the public interest is balanced with privacy and safety concerns, which are of the utmost importance, it is key that the unique factors connected to this section are considered – this will ensure that disclosure decisions are made in a way that reflects the unique nature of workplace investigation records.

This would also ensure that considerations of privacy and harm (s.37 and s.40), which are of the utmost importance, remain protected and still achieve the overall intent of this recommendation.

Suggestion: Modify recommendation to require mandatory disclosure of the final report with limited exceptions relating to s.40 and s.37. Furthermore, provide the public interest consideration within s.33 rather than s.9.

---

vii) Intergovernmental relations

#	2020 Recommendation (summary)	Notes
45.	That the **Act** be amended to extend the intergovernmental relations exception to all Indigenous self-governing bodies.	Government is supportive of this recommendation.

viii) Conservation

#	2020 Recommendation (summary)	Notes
46.	That the **Act** be amended to extend the harm-based exception to information about species and populations which the head of a public body has reasonable grounds to believe are in need of protection.	Government is supportive of this recommendation.

ix) Third party commercial interests

#	2020 Recommendation (summary)	Notes
47.	Remove the requirement that information has to have been supplied in confidence from the exception for disclosure harmful to third parties' business interests.	Government is supportive of this recommendation.
48.	Provide a mandatory exception for trade secrets.	Government is supportive of this recommendation.
49.	Provide a 20-year sunset clause on third-party business information.	Government is supportive of this recommendation.
50.	Make the exception for disclosure harmful to third parties' business interests subject to the public interest override.	Government is supportive of this recommendation with modification. See commentary below.

Recommendation 50 (make exception for disclosure to third party business interest subject to the public interest override)

Issue:
In 2015 the **Act** was amended to include a public interest override for most discretionary exceptions after the 2014 ATIPPA review. In their final report, the Committee outlined what they had heard from various stakeholders. Included was the Centre for Law and Democracy's recommendation that "the public interest override apply to both discretionary and mandatory exceptions…" After extensive research, both nationally and internationally, the Committee chose to exclude limited discretionary exceptions and all mandatory exceptions from the public interest override.

In the final report of the 2020 review, the Committee recommended that only one mandatory exception be added to the public interest override – s.39, as it relates "to the economic activities of government, whether as purchaser, investor or otherwise, and whether direct or through an intermediary." The Chair further wrote:

> Making these exceptions subject to a public interest override will not affect the substantive aspects or nature of the exception, but will require the public interest in disclosure to prevail when circumstances tip the scales in favour of disclosure. One may ask the simple question – 'why should this not be the case?' – I have not been given a persuasive response.

Government supports the spirit of this recommendation and agrees that there should be an ability to disclose information that falls under s.39 where there is a public interest. In reviewing other legislation within Canada where equivalent s.39 exceptions fall within a comparable public interest override, six fall under the broader override that applies to all exceptions (Nova Scotia, Prince Edward Island, Ontario, Alberta, British Columbia, Northwest Territories) while four have a public interest override within the exception New Brunswick, Manitoba, Saskatchewan, Canada). Additionally, the Yukon's **Access to Information and Protection of Privacy Act** has a hybrid approach – while the exception for third party business information falls within the broader public interest override under section 82 , there are provisions specific to s.69 (third party business information within this section outlining factors to consider when determining if the public interest override applies:

> (b) if the information is of a type referred to in paragraph 69(1)(a) or (b), the head must consider the following factors in addition to the factors referred to in paragraph (a):
> (i) whether the public interest in disclosing the information clearly outweighs
> (A) any financial loss or gain to a person or entity that could be reasonably expected to occur because of the disclosure, or
> (B) any harm to the competitive or negotiating position of a person or entity that could be reasonably expected to occur because of the disclosure,
> (ii) whether disclosing the information could be reasonably expected to improve competition; and
> (c) the head must not consider the following factors:
> (i) the applicant's identity or motive for requesting access to the information,
> (ii) whether the medium in which the information is available would, if the information were disclosed in that medium, contribute to misunderstanding of the information by the applicant or the public,
> (iii) whether there are means, other than through submitting an access request, for the applicant or the public to become aware of the information or know that it exists.

As it relates to the jurisdictions where third party business information falls under the broader public interest override, other than Ontario, all have prescriptive processes in place:

- Must notify third parties – Nova Scotia
- Must notify third parties and provide opportunity for them to provide representations regarding the disclosure – Prince Edward Island, Alberta, British Columbia, Northwest Territories

In Newfoundland and Labrador, similar provisions are not found within section 9 of the **Act** – perhaps because it currently only applies to discretionary exceptions to disclosure. If the **Act** were amended to include a mandatory exception to disclosure under section 9, it would likely also require amendments similar to other jurisdictions requiring notification and opportunity for third parties to provide representations, which would have broader implications for the section.

Given the above, it is suggested that the public interest override falls within s.39 rather than s.9 of the **Act**. This would be in line with other mandatory exceptions such as section 40 (personal information) that does not fall under the broader section 9 public interest override but would still achieve the overall intent of this recommendation, while limiting the broader changes to section 9 that may be required if a mandatory exception to disclosure were to be added.

Suggestion: Modify the recommendation to include public interest override under s.39 rather than s.9 of the **Act**.

---

x) Third party notification

#	2020 Recommendation (summary)	Notes
51.	Allow public bodies to consult with third parties while considering requests for information the release of which might be harmful to their interests.	Government is supportive of this recommendation
52.	Require a third party who files a complaint or an appeal to provide a copy of the complaint or notice of appeal to the public body.	Government is supportive of this recommendation.

xi) Information technology security

#	2020 Recommendation (summary)	Notes
53.	That the **Act** be amended to provide a discretionary harm-based exception to access for information technology security information.	Government is supportive of this recommendation.

#	2020 Recommendation (summary)	Notes
54.	That the OCIO and the ATIPP Office provide to the smaller public bodies basic information and guidance on the types of information technology security information and the records which may contain such information.	Government is supportive of this recommendation.

xii) Testing procedures and audits

#	2020 Recommendation (summary)	Notes
55.	That the **Act** be amended to provide a discretionary harm-based exception to access for test-related information.	Government is supportive of this recommendation; however, suggest further review of whether to repeal paragraph 5(1)(f) depending on potential impacts to public bodies such as the Public Service Commission, NL Schools, and the Conseil scolaire francophone provincial de Terre-Neuve-et-Labrador to ensure no unintended consequences.

1.11 Public interest override

#	2020 Recommendation (summary)	Notes
56.	That the **Act** be amended to extend the public interest override to all discretionary exceptions, to third party commercial interests, and to the final report of a workplace investigation.	See commentary below.

Recommendation 56 (public interest override)

Issue:
Two of the exceptions referred to in Recommendation 56 are mandatory exceptions for third party business interests (s.39) and workplace investigations (s.33).

Section 9 establishes that information subject to a discretionary exception can be released where it is in the public interest. Currently, the public interest override applies to discretionary exceptions other than exceptions related to law enforcement and individual/public safety. It does not apply to any mandatory exceptions (cabinet confidences has its own discretionary public interest override in section 27; personal information also has a public scrutiny

consideration in s.40(5)(a)). Government is supportive of extending the public interest override to all discretionary exceptions. However, it is suggesting that the recommendation be modified as it relates to the mandatory exceptions cited – the public interest override should be added directly to sections 33 (workplace investigations) and 39 (third-party information) versus section 9 of the **Act**. This would reflect the difference between mandatory and discretionary exceptions, as well as be consistent with other public interest overrides currently found within mandatory exceptions of the Act.

Suggestion: Add a public interest override within the section governing a mandatory exception, specifically ss.39 and 33, which is more consistent with the public interest override consideration related to cabinet confidences under s.27.

1.12 Sunset clauses

#	2020 Recommendation (summary)	Notes
57.	That the **Act** be amended to replace the 50-year sunset clause on archived records in sections 38 and 39 with a 20-year sunset clause with no reference to archived records.	Government is supportive of this recommendation.

1.13 Veterinary Medical Association

#	2020 Recommendation (summary)	Notes
58.	That the **Act** be amended to exclude treatment records created by a public body veterinarian for fee for service treatment that would not otherwise be provided by a public body veterinarian if a private veterinarian were available.	Government is supportive of this recommendation.

1.14 Submissions of the Office of the Speaker of the House of Assembly

#	2020 Recommendation (summary)	Notes
59.	Provide the Lieutenant-Governor-in-Council with the authority to recommend additions to Schedule B.	Government is supportive of this recommendation.
60.	Require the Selection Committee to provide no more than three candidate names to the Speaker when choosing a new commissioner.	See commentary below.

#	2020 Recommendation (summary)	Notes
61.	Give the formal responsibility for bringing forward the resolution naming a new commissioner to the government House Leader.	See commentary below.
	Suggestion 2: That any disclosure by the Speaker of the names of the recommended candidates during the consultation process, and any subsequent sharing of those names by the party leaders with their members, be on the clear understanding and expectation of confidentiality. That consideration be given to including a definition of "sitting of the House of Assembly" when used in the legislation respecting statutory offices, including **ATIPPA, 2015**.	See commentary below.

Recommendations 60, 61 and Suggestion 2 (appointment of the Commissioner)

Issue:
The 2014 statutory review considered the appointment process for the Information and Privacy Commissioner in the context of independence, transparency and public confidence. The Committee's objective was to strengthen the perceived and actual independence of the Commissioner by ensuring that appointments were informed by a merit-based selection process and that leading candidates would be identified through a selection committee before consideration by the House of Assembly. This approach reflected the broader purpose of the **Act**, which was to enhance the role and independence of the Commissioner following the review.

However, since that time, government established the Independent Appointments Commission (IAC). The IAC was established in 2016 as "an independent, non-partisan body to provide merit-based recommendations of qualified individuals for appointment to those provincial Agencies, Boards and Commissions (ABCs) listed in the schedule to the **Independent Appointments Commission Act**." Of the seven statutory officers of the House of Assembly, six are appointed through the IAC process. The only officer that is not appointed through the IAC is the Information and Privacy Commissioner.

In 2023, the Honourable Robert Fowler released his report, Structural Review of the Statutory Offices of the House of Assembly. This review focused on the structure or administration of these offices, including how each statutory officer should be recruited, appointed, re-appointed, compensated, disciplined, and removed from office."

During his review, Justice Fowler heard from various stakeholders including the former Information and Privacy Commissioner. In reviewing the different appointment processes, he identified issues with all. Despite concerns outlined, he concluded that he saw "no reason why the same process cannot be applied to all statutory officer appointments."

It is government's position that the appointment process for all statutory officers should follow a consistent appointment framework which would promote clarity, reduce unnecessary differences between statutory offices, and reinforce that the Information and Privacy Commissioner is part of the same independent accountability framework as other officers of the House of Assembly, such as the Auditor General.

For this reason, the recommendation can be reframed from creating or maintaining a separate appointment process in the **Act** to ensuring that the Commissioner's appointment process is addressed through the same legislative and procedural framework that applies to other statutory officers, while maintaining appropriate safeguards for independence, merit and confidentiality.

Suggestion: Consider removing the appointment process from the **Act** and aligning the Commissioner's appointment process with the legislative and procedural framework used for other statutory offices of the House of Assembly.

1.15 Submissions of the Statutory Offices of the House of Assembly

#	2020 Recommendation (summary)	Notes
62.	Make clear that the exception to disclosure for statutory office records extends to those offices' audit functions.	Government is supportive of this recommendation.
63.	Make the Office of the Auditor General subject to **ATIPPA, 2015**.	Government is supportive of this recommendation. See commentary below.

Recommendation 63 (Auditor General subject to ATIPPA, 2015)

Issue:
The Office of the Auditor General is one of seven statutory offices of the House of Assembly. It is currently the only statutory office that is not subject to the **Act**.

Justice Orsborn specifically considered the inclusion of the Auditor General under the scope of the **Act**. In his discussion of the issue, Justice Orsborn cited the 2007 report by Chief Justice J. Derek Green, Rebuilding Confidence. In that report, Justice Green recognized the unique function of the Auditor General and the importance of ensuring the protection of records and reports relating to its statutory obligations. Justice Green went on to state that:

> "[…] there is no reason why general financial and other information about the operation of the offices themselves and the expenses of the heads of the offices and the staff should not be available.
>
> […] I believe a case can be made for subjecting the Auditor General to basic access to information requirements about the financial and administrative organization of the office."

Justice Orsborn agreed with Justice Green that the Auditor General should be included as a public body under the **Act** but to ensure that records connected with the investigative or audit functions be protected from access to information requests.

While the discussion by Chief Justice Green and Justice Orsborn focused on the right of access to basic financial and administrative information related to the Auditor General, government would also note that the current exclusion of the Audit General also means that there is no legislative regime governing the handling of personal information that is collected, used, disclosed, stored or destroyed by that office. Including the Auditor General as a public body under the **Act** would provide a clear and legislative requirement to ensure the protection of personal information in its custody or control.

Suggestion: Make the Office of the Auditor General a public body under the **Act** while clearly excepting statutory office records, including audit functions, from disclosure under the **Act**. In addition, make the Office of the Auditor General subject to the privacy provisions of the **Act**.

1.16 Office of the Information and Privacy Commissioner

i) Vacancy in the Office of the Information and Privacy Commissioner

#	2020 Recommendation (summary)	Notes
64.	That the **Act** be amended to allow the commissioner to designate a person who will assume their powers and duties in the event of their absence or a vacancy in the office of commissioner	See commentary below.

Recommendation 64 (commissioner designate)

<u>Vacancy in the office of commissioner:</u>
Section 89 of the **Act** provides the mechanism for appointment of an acting commissioner where the Commissioner is unable to perform their duties or the position becomes vacant. This allows the Lieutenant Governor in Council (LGIC), on recommendation of the House of Assembly Management Commission, to appoint an acting commissioner in certain circumstances.

There currently exists a process to allow for the appointment of an acting commissioner. Section 89 states:

> 89. (1) The Lieutenant-Governor in Council may, on the recommendation of the House of Assembly Management Commission, appoint an acting commissioner if
>
> (a) the commissioner is temporarily unable to perform his or her duties;
>
> (b) the office of the commissioner becomes vacant or the commissioner is suspended when the House of Assembly is not in session; or
>
> (c) the office of the commissioner becomes vacant or the commissioner is suspended when the House of Assembly is in session, but the House of Assembly does not pass a resolution to fill the office of the commissioner before the end of the session.

This is consistent with all other jurisdictions within Canada. During the 2015 statutory review, the process for selecting the information and privacy commissioner was an area of focus. Specifically, the committee commented,

> "[…] the perception of a Commissioner who is independent from government would be greatly enhanced if the choice resulted from efforts by a selection committee that would identify leading candidates for consideration."

Changing this approach would be a departure within Canada and poses potential concerns regarding the impartiality and merit-based process that was intended to be achieved by the process established with the introduction of s.89 of the **Act**.

Suggestion: No change is required to the **Act**. There already exists a process for appointing an acting commissioner where the position of commissioner is vacant.

Absence in the office of the commissioner:

Section 103 of the **Act** provides the commissioner with the authority to delegate a duty or power under the Act to a person on the staff of the commissioner. This allows for the commissioner to delegate to a staff member where they will be absent (e.g. on vacation).

Suggestion: No change is required to the **Act** as the authority already exists within the **Act** to address the situation where the commissioner is absent from the office.

---

ii) The Office of the Information and Privacy Commissioner as a public body

#	2020 Recommendation (summary)	Notes
65.	That the **Act** be amended to provide that where the OIPC is responding to a request in its capacity as a public body, procedural or administrative matters that would otherwise be referred to the OIPC be referred to the Office of the Citizens' Representative and that matters requiring a level of adjudication be referred to the Supreme Court.	Government is supportive of this recommendation.

iii) Compellability of OIPC personnel as witnesses

#	2020 Recommendation (summary)	Notes
66.	That the **Act** be amended to remove the non-compellability of OIPC personnel as witnesses in proceedings involving an offence under the **Act** or a charge of perjury.	Government is supportive of this recommendation.

iv) OIPC investigations and s.8.1 of the Evidence Act

#	2020 Recommendation (summary)	Notes
67.	That the **Act** be amended to repeal section 101.	Government is supportive of this recommendation.

1.17 Municipalities

#	2020 Recommendation (summary)	Notes
68.	Provide that only one person can be designated as the head of a local public body.	Government is supportive of this recommendation with modifications.
69.	Allow local public bodies to designate a person not on staff as a coordinator or as the head of the public body under exceptional circumstances, when approved by the commissioner.	Government is supportive of this recommendation with modifications.
70.	That Government develop a cost-reimbursement process whereby municipalities established under the **Municipalities Act, 1999** may be reimbursed for all or a portion of the marginal costs incurred in responding to ATIPP requests.	See commentary below.
71.	That Government establish a Municipality ATIPP Team to determine and review as required the resources reasonably needed by municipalities to administer ATIPP in each municipality.	Government is supportive of this recommendation.

Recommendation 70 (cost reimbursement for municipalities)

Issue:
There have been a number of steps taken in the last one to two years to increase ATIPP-related supports for municipalities. This includes adding additional municipal access and privacy analyst positions within the ATIPP Office to provide more dedicated support to municipalities, as well as enhancing training and guidance available to municipal public bodies. These measures recognize that municipalities vary significantly in size, staffing, resources, and information management capacity, and that many smaller municipalities may require more practical, targeted, and ongoing support to meet their obligations under the **Act**.

A review of access to information requests since 2005-06 for cities and municipalities highlights how request trends and volumes fluctuate significantly for a number of municipalities each year. There has been a significant increase in the number of requests received by municipalities overall in the past three to four fiscal years.

Fiscal year	General	Personal	Combined	*Monthly average*
2005-06	18	3	21	*1.8*
2006-07	31	6	37	*3.1*
2007-08	65	6	71	*5.9*
2008-09	73	7	80	*6.7*
2009-10	88	6	94	*7.8*
2010-11	78	5	83	*6.9*
2011-12	58	10	68	*5.7*
2012-13	80	12	92	*7.7*
2013-14	62	4	66	*5.5*
2014-15	91	6	97	*8.1*
2015-16	188	12	200	*16.7*
2016-17	286	22	308	*25.7*
2017-18	441	9	450	*37.5*
2018-19	302	11	313	*26.1*
2019-20	292	11	303	*25.3*
2020-21	373	23	396	*33.0*
2021-22	308	18	326	*27.2*
2022-23	422	34	456	*38.0*
2023-24	625	34	659	*54.9*
2024-25	711	21	732	*61.0*
2025-26*	498	24	522	*43.5*
2026-27**	370	24	394	*65.7*

**These statistics are initial estimates and not official figures.*
***Statistics as of September 30, 2026*

While these supports are important, further work is required to better understand the specific needs of municipalities and to ensure that available resources are directed in the most effective way. A one-size-fits-all approach may not adequately reflect the operational realities of municipalities, particularly those with limited administrative capacity or limited access to dedicated information management, legal, or privacy expertise.

Although smaller municipalities may face resource challenges when processing access requests, the potential demand, administrative requirements, eligibility criteria, and costs of a reimbursement program are unclear.

Given the proposed changes to the cost schedule, which may reduce the number, scope, or complexity of requests, together with the additional ATIPP Office resources now in place to support municipalities and the creation of a municipal ATIPP team, it is recommended that government first monitor municipal ATIPP demands and needs before determining whether additional resources are required. The municipal ATIPP team can assess emerging access and privacy needs and identify appropriate supports or resource requirements based on that experience.

Suggestion: Monitor the impact of the proposed cost schedule changes, additional ATIPP Office resources, and the municipal ATIPP team before determining what municipal supports or resources are required. This will allow municipal access and privacy demands to be assessed based on actual needs and experience.

1.18 Recommendations 4 and 16 of the Muskrat Falls Inquiry

#	2020 Recommendation (summary)	Notes
72.	Provide that a public inquiry is not a public body for ATIPP purposes.	Government is supportive of this recommendation.
73.	Include s. 28 of the **Public Inquiries Act, 2006** in Schedule A.	Government is supportive of this recommendation.
	Suggestion 3: That government consider amending the **Energy Corporation Act** to provide that the corporation is required to provide to the responsible minister such information as may be requested by the minister.	This recommendation is no longer required. The **Energy Corporation Act** was repealed and replaced with the **Hydro Corporation Act, 2024** which includes section 30 - "Where requested by the minister, the corporation or a subsidiary shall provide the minister with the information, records, reports and other documents the minister specifies in the request relating to the business and affairs of the corporation or the subsidiary."

1.19 Publication schemes, information directories and proactive disclosure

#	2020 Recommendation (summary)	Notes
74.	Require the creation of publication schemes by all public bodies other than small municipalities and others exempted by regulation.	See commentary below.
75.	Require public bodies other than local public bodies to develop and publish categories of records and information that will be published routinely.	Government is supportive of excluding local public bodies, particularly municipalities from this recommendation. See further commentary below regarding the remainder of the recommendation.
76.	Provide that the categories for proactive disclosure will include ministerial briefing notes, executive travel expense reports, records presently listed in paragraphs 29(2)(b) to (k), and others specified by regulation.	See commentary below.
77.	Allow the commissioner to comment on and recommend improvements to publication schemes and proactive disclosure.	See commentary below.
78.	Delay the coming into effect of the publication scheme and proactive disclosure provisions until January 1, 2023.	Government is supportive of a delayed coming into force of the requirements surrounding publication schemes and proactive disclosure.
79.	That public bodies should complete a proposed publication scheme and submit it to the OIPC for review and comment prior to the requirement coming into force	See commentary below.

Recommendation 74 (publication schemes)

Issue:
Government recognizes the importance of making as much information available as possible without the need for formal access to information requests. It is also important that the public understands the role and function of each public body to know what information it may hold. In recognition of this important undertaking, government is proposing amendments to section 110 to better achieve the objective of providing the public with information about the mandates of public bodies and what information it holds/relies upon to deliver on that mandate.

Government would look to other jurisdictions who have adopted a public-focused approach to making information available to the public. Five Canadian jurisdictions do not specify in their respective Acts what information must be publicly available without a formal access to information request but rather permit the head of a public body (or the minister responsible for their Act) to specify categories of records that are publicly available without a request (British Columbia, Alberta, Saskatchewan, Manitoba, Prince Edward Island). British Columbia's **Freedom of Information and Protection of Privacy Act** sets out that the minister may establish categories of records that are available to the public without requiring an access request (s.71.1) and has issued Ministerial directives for the release of government information.

The United Kingdom's **Freedom of Information Act 2000** requires that every public authority adopt and maintain a publication scheme, publish information in accordance with its scheme and from time to time review its scheme. The UK Information Commissioner developed a model publication scheme to be adopted by public bodies. It focuses on seven major components:

- **Who we are and what we do**. Organizational information, locations and contacts, constitutional and legal governance.
- **What we spend and how we spend it**. Financial information relating to projected and actual income and expenditure, tendering, procurement and contracts.
- **What our priorities are and how we are doing**. Strategy and performance information, plans, assessments, inspections and reviews.
- **How we make decisions**. Policy proposals and decisions. Decision making processes, internal criteria and procedures, consultations.
- **Our policies and procedures**. Current listing of policies and processes for delivering our public functions and responsibilities.
- **Lists and registers**. Information held in registers required by law and other lists and registers relating to the functions of the authority.
- **The services we offer**. Advice and guidance, booklets and leaflets, transactions and media releases. A description of the services offered.

A current review of departmental websites indicates that a fair amount of these categories of information are already available on departmental websites, such as **who we are and what we do**; **what our priorities are and how we are doing** by way of things like strategic plans and annual performance reports; **policies and procedures**; and, **services we offer**.

Other categories of information may be more dependent on the mandate of the department (e.g. lists and registers). What we spend and how we spend it is generally captured in annual budget and expenditure information. Additional expenditure information such as tendering and procurement information is handled and published through a central system (MERX).

Government also supports Orsborn's recommendation to exclude small municipalities and other public bodies exempt by regulation. This recognizes the unique circumstances faced by many small municipalities with limited resources.

Suggestion: Consider whether s.110 should be amended to specify the main categories of information that must be published on each department's website, similar to the UK's publication scheme requirement.

Recommendations 75 and 76 (requirement and categories for proactive disclosure)

Issue:
Government is supportive of proactive disclosure requirements that support openness and transparency, while recognizing that resources vary across public bodies, particularly municipalities. However, the proposed records set out under s.29(2)(b) – (k) encompass a broad scope of records (e.g. factual material, etc.) and may continue to be subject to other statutory exceptions to disclosure. Consequently, proactive release would require case-by-case review and redaction to ensure compliance with the **Act**. Requiring the proactive disclosure of such a broad scope of records that would require line-by-line review would not be feasible. The associated resource requirements would be significant and would likely outweigh the benefits of mandatory disclosure of these categories.

Each category of records requires careful analysis and consideration to assess whether such records can be easily disclosed without the need for line-by-line review, redactions or consultations.

British Columbia's **Freedom of Information and Protection of Privacy Act ("FOIPPA")** includes a provision for government-wide disclosure of records by allowing the Minister responsible for the Act to establish categories of records available without an access request. Specifically, s.71.1 states:

> **71.1**(1) Subject to subsection (2), the minister responsible for this Act may establish categories of records that are in the custody or under the control of one or more ministries and that, without a request for access under this Act,
>
> (a) are available to the public, or
>
> (b) in the case of a record that contains personal information about an individual, a ministry may make available to the individual.
>
> (2) The minister responsible for this Act must not establish a category of records that contain personal information unless the information
>
> (a) may be disclosed under section 33, or
>
> (b) would not constitute, if disclosed, an unreasonable invasion of the personal privacy of the individual the information is about.
>
> (3) Section 22 (2) to (4) applies to the determination of unreasonable invasion of personal privacy under subsection (2) (b) of this section.
>
> (4) The minister responsible for this Act may require one or more ministries to disclose a record that is within a category of records established under subsection (1) of this section or section 71 (1).
>
> (5) If required to disclose a record under subsection (4), a ministry must do so in accordance with any directions issued relating to the disclosure by the minister responsible for this Act.

(6) The head of a public body may sever from a record made available under this section any information the head of the public body would be entitled under Part 2 of this Act to refuse to disclose to an applicant.

(7) If information is severed from a record, the record must include a statement of

(a) the fact that information has been severed from the record,

(b) the nature of the information severed from the record, and

(c) the reason for severing the information from the record.

Alberta's **Protection of Personal Information Act ("POPA")** also contains a provision that allows the head of a public body to specify categories of records that are available without an access request. This would enable a public body to identify its own unique records that are available without a request and that which would not be appropriate for a government-wide disclosure (e.g. the Department of Government Services proactively publishes restaurant inspection reports). Section 90 of Alberta's **POPA** states:

90(1) The head of a public body may specify categories of records that are in the custody or under the control of the public body and are available to the public without a request for access under this Act.

(2) Any information that the head of a public body would be authorized or required to refuse to give access to under this Act may be excluded from a record that is available to the public without a request for access under this Act.

(3) The head of a public body may require a person who asks for a copy of an available record to pay a fee to the public body, unless such a record can otherwise be accessed without a fee.

(4) Subsection (1) does not limit the discretion of the Government of Alberta or a public body to release records that do not contain personal information.

(5) Despite anything to the contrary in this Act, there is no right to request a review in relation to a decision respecting whether to make a record available to the public under this section.

Suggestion: Rather than prescribing broad categories of records for proactive disclosure, consideration could be given to establishing proactive disclosure requirements of specific types of records that can reasonably be disclosed without extensive review. For government-wide disclosure of records, consider establishing an approach similar to British Columbia's **FOIPPA** s.71.1.

For other records which are more specific to a particular department, consider establishing a provision similar to Alberta's s.90 of **POPA** that would allow the head of a public body to specify records that are available without a request for access. This would allow the head to designate specific categories of records within their public body for proactive disclosure (e.g. completed access to information requests are released proactively by the ATIPP Office; restaurant inspection reports are proactively released by the Department of Government Services, etc.).

Recommendation 77 (commissioner comment on publication schemes and proactive disclosures)

Issue:
The objectives of this recommendation can largely be achieved through the Commissioner's existing mandate. Section 95 of the **Act** provides broad authority to comment on matters affecting access to information and privacy, which would encompass issues relating to publication schemes and proactive disclosure initiatives. Given these existing oversight mechanisms, it is not clear that an additional express authority would provide significant added value. Maintaining the current framework would avoid unnecessary duplication while preserving the Commissioner's ability to offer observations and recommendations in this area.

Suggestion: Consider maintaining the current approach as set out under s.95.

Recommendation 79 (submit proposed publication schemes to OIPC for review and comment)

Issue:
The proposed approach related to recommendation 75 contemplates prescribing the content of publication schemes directly in section 111, providing public bodies with clear legislative direction regarding what must be included. As a result, publication schemes would be developed based on statutory requirements rather than a template or guidance document prepared by the OIPC. In addition, the Commissioner already has broad oversight and auditing powers that would permit the review of publication schemes where concerns are identified or where such review is otherwise warranted. Given these existing mechanisms and government's red tape reduction efforts to streamline processes, a requirement for all public bodies to submit proposed publication schemes for review before they come into force would introduce an additional administrative step without a corresponding benefit to transparency or accountability, given the Commissioner's existing broad oversight powers.

Suggestion: Consider amending section 111 with a prescribed list of information to be included in a publication scheme, removing the administrative burden associated with an additional review process prior to publication.

1.20 Protection of privacy

i) Policies and procedures

#	2020 Recommendation (summary)	Notes
80.	That the **Act** be amended to require a public body to develop and publish policies and procedures for the protection of personal information.	Government is supportive of this recommendation with modification.

Recommendation 80 (develop and publish privacy protection policies)

Issue:
Policies and procedures are important tools for public bodies when processing personal information, ensuring that processes are clear, that authority is well-established and that any personal information is protected. From the perspective of transparency, it is also important that information be available to individuals regarding how their personal information is collected, used and disclosed.

Provinces vary in their requirements to create and publish policies. Most provinces include at least some requirements to make policies available. A number including New Brunswick, Quebec, Nova Scotia, Manitoba, and Saskatchewan also have varying obligations to create policies to protect personal information.

New Brunswick has a particularly strong section in this regard, requiring public bodies to establish "information practices" if they are using personal information to make a decision about someone and to make information available to the public about those practices.

Public bodies should, however, be aware that for some information, publishing too much detail could create a cybersecurity risk if it would reveal how to access a system or where weaknesses may lie. For this reason, public bodies should have some flexibility to withhold information that would create such a risk. For example, Saskatchewan's **Freedom of Information and Protection of Privacy Act** section 24.1 requires the publication of policies and manuals but also states:

> (2) Any information in a record that a head would be authorized to refuse to give access to pursuant to this Act or the regulations may be excluded from manuals, policies, guidelines or procedures that are made available or provided pursuant to subsection (1).

Suggestion: Amend the Act to require public bodies to:

- establish policies and procedures when personal information is used to make decisions affecting individuals; and
- publish relevant policies, subject to limited redactions where disclosure would create an unreasonable security risk.

ii) Privacy impact assessments

#	2020 Recommendation (summary)	Notes
81.	Define "common or integrated program or service".	Government is supportive of this recommendation.
82.	Require non-departmental public bodies to prepare preliminary assessments and, if required, privacy impact assessments, with the option of submitting them to the commissioner for review and comment.	Government is supportive of this recommendation with modifications. See commentary below.

#	2020 Recommendation (summary)	Notes
83.	Specify that the commissioner has the authority to monitor compliance with the requirement to conduct privacy assessments and to make recommendations for improvement	See commentary below.
84.	That privacy impact assessments received by heads of non-departmental public bodies may optionally be also sent to the ATIPP Office for review and comment.	Government is supportive of this recommendation.
	Suggestion 4: That smaller public bodies seek guidance from the ATIPP Office and the OIPC as needed when considering the privacy impacts of any program or service. That a public body developing a common or integrated program or service should consider both notifying the ATIPP Office at an early stage of the development of the program or service and also submitting the PIA to that office for its review and comment.	Government is supportive of this recommendation.

Recommendation 82 (privacy impact assessments for public bodies)

Issue:
Currently only departments are required to complete privacy assessments under the **Act**. Extending this requirement to other public bodies will have a resource impact on those public bodies. However, it would also improve compliance with privacy provisions under the **Act** and requires that privacy is considered during the development of any programs or services.

Suggestion: The requirement should apply to all public bodies, but implementation for local government bodies should be delayed, allowing time for the municipal ATIPP team to assess the privacy needs of towns and cities and establish a process to support them in undertaking privacy assessments. The **Act** should also establish when an assessment must be submitted to the Office of the Information and Privacy Commissioner, with consideration given to a risk-based submission threshold as set out in section 3.4 of this document.

Recommendation 83 (commissioner monitor compliance with privacy assessment requirements)

Issue:
The Office of the Information and Privacy Commissioner already has broad authority under the Act to monitor compliance and audit the practices and procedures of public bodies. Specifically, section 95(1)(b) gives the Commissioner authority to:

> (b) monitor and audit the practices and procedures employed by public bodies in carrying out their responsibilities and duties under this Act; [section 95(1)(b)]

This would cover compliance with provisions around privacy impact assessments. A jurisdictional review of other provinces did not reveal a provision similar to the ones suggested.

Suggestion: No change is required to the **Act** as the Commissioner already has broad authority to monitor compliance under s.95(1)(b).

---

iii) Information sharing agreements

#	2020 Recommendation (summary)	Notes
85.	That in the course of conducting a privacy impact assessment involving a common or integrated program or service, public bodies consider whether an information sharing agreement is reasonably required for the protection of personal information the disclosure of which may be permitted under paragraph 68(1)(u).	Government is supportive of this recommendation.

iv) Artificial intelligence

#	2020 Recommendation (summary)	Notes
86a	Define "algorithmic impact assessments" and require that any public body planning to implement an automated decision system complete one and, if requested, provide it to the commissioner.	See commentary below.
86b	Define "automated decision system".	See commentary below.
87.	Require that public bodies notify the commissioner when developing a program or service using automated decision systems.	See commentary below.

#	2020 Recommendation (summary)	Notes
88.	Require public bodies to keep records of the decision-making processes of automated decision systems.	See commentary below.
89.	Include monitoring and commenting on automated decision systems in the general powers and duties of the commissioner.	See commentary below.

Recommendation 86(b) (definition of automated decision system)

Issue:
Currently, no provincial privacy legislation contains a definition of an "automated decision system," though Quebec, Alberta and British Columbia each have legislation that refers to these systems. The committee for the 2020 review recommended the following definition:

> "automated decision system means any technology that assists or replaces the judgement of human decision-makers using techniques such as rules-based systems, regression analysis, predictive analytics, machine learning, deep learning, neural networks, and artificial intelligence."

This definition is very similar to the definition contained in Canada's Bill C-27 (**Digital Charter Implementation Act, 2022**), which did not proceed. It stated:

> "automated decision system" means any technology that assists or replaces the judgment of human decision makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique.

The Government of Canada introduced Bill C-36 at first reading on June 15, 2026, an Act to enact the **Protecting Privacy and Consumer Data Act** which would replace Part 1 of the **Personal Information Protection and Electronic Documents Act**. This Bill includes a definition of "automated decision system" which is substantially similar to the definition found in Bill C-27:

> **automated decision system** means any technology that assists or replaces the judgment of human decision-makers through the use of a rules-based system, regression analysis, predictive analytics, machine learning, deep learning, a neural network or other technique.

Given the changing technology, there are challenges trying to clearly define what is meant; the techniques may change and evolve over time. It may be appropriate to include some flexibility in the definition to allow for different techniques; perhaps

> "Automated decision system means any technology that assists or replaces the judgement of human decision-makers using techniques **including but not limited** to rules-based systems, regression analysis, predictive analytics, machine learning, deep learning, neural networks, and artificial intelligence."

Previously, concerns were raised about the definition and the potential of over-breadth (e.g., a system that automatically sends a permit application to the correct person, department, or workflow based on pre-set rules). The language in **Bill C-36** would mean that obligations would attach only where an automated decision system is used to assist or make a decision about an identifiable individual using their personal information. As such, routing, formatting, and calculation functions would fall outside this obligation because they do not evaluate or make inferences about a person.

Suggestion: Consider including a definition of "automated decision making" in the **Act** similar to the definition in Canada's **Bill C-36** and clarifying that requirements should apply only when a system uses someone's personal information to make, or play a substantial role in making, a decision that affects their legal rights or has a similarly significant impact on them. Consider whether to include a provision that confirms that the definition does not apply to systems routing information, formatting documents, or other administrative functions that do not evaluate, score, or make inferences about an individual. Further, consider including any such definition under Regulations to allow for more efficient and adaptable definitions and processes that reflect the fast-changing technology landscape.

Recommendation 86 (define algorithmic impact assessment)

Issue:
Like "automated decision making", there are challenges with defining this term. There currently is no definition of "algorithmic impact assessment" that has been adapted into Canadian legislation. The Government of Canada has defined this term in its **Directive on Automated Decision-Making**:

> "A framework to help departments better understand and reduce the risks associated with automated decision systems and to provide the appropriate requirements that best match the type of system being designed."

Topics covered in an algorithmic impact assessment (AI assessment) include the following, some of which may not necessarily be included in a privacy assessment:

- Purpose for the AI system
- Parties involved in designing the system
- Data source
- Validity and bias
- Impact on individuals or communities
- Harm mitigation strategies
- Explainability
- Human-in-the-loop
- Testing/reporting/ongoing evaluation

These topics have significant overlap with privacy assessments but also contain analysis that is unique from privacy assessments. Additionally, AI assessments may also be carried out on programs or services that do not involve personal information or have any privacy implications.

As this is a quickly changing area, it is recommended that standards for the form and content of algorithmic impact assessments should be set out by regulation. The role of regulation in setting these standards in the face of technological change is set out at Section 3.2 – Making the Act flexible as technology evolves.

The Office of the Chief Information Officer has developed and implemented AI assessments that departments are required to complete when a project uses artificial intelligence. These assessments are then reviewed by various groups, including the OCIO, the ATIPP Office (where it involves personal information) and an Executive Oversight Committee to consider the broader issues associated with automated decision-making systems. These systems pose unique challenges and should be effectively addressed. Having a definition in the **Act** of what is an algorithmic impact assessment would be beneficial. In addition, setting out a requirement in the **Act** to undertake such an assessment before using an automated decision system involving personal information would strengthen privacy protections. The specific standards on what should be included in such an assessment, when an assessment is required and what is deemed to be low, medium, high or unacceptable risk associated with the proposed system should be set out in Regulations to allow for more efficient and adaptable definitions and processes that reflect the fast-changing technology landscape.

Suggestion: Consider including a definition of algorithmic impact assessment into the **Act**.

Recommendation 87 (notify commissioner when developing a program/service using automated decision systems)

Issue:
The Orsborn review recommended that the **Act** be amended to require public bodies to notify the Commissioner when developing a new program or service using automated decision making. This recommendation would result in a significant expansion of the mandate of the Office of the Information and Privacy Commissioner. Currently, the duties of the Commissioner are set out in section 95 of the **Act** and relate specifically to access to information and protection of privacy. Some projects that use automated decision making do not involve privacy or access implications; giving the Commissioner a mandate to review such projects would expand beyond the statutory function of this office and introduce additional administrative burden for public bodies.

However, automated decision systems can have significant implications for privacy, access to information, and the rights of affected individuals. A risk-based approach to OIPC notification on privacy assessments would be most appropriate, particularly in the absence of a larger AI regulatory framework. Under this approach, notification to the OIPC would be required where a privacy assessment identifies a significant risk to privacy or access, while low- and medium-risk uses would not automatically trigger notification.

This approach would preserve meaningful oversight for the highest-risk uses where it impacts privacy or access rights without requiring the Commissioner's involvement in every AI-related initiative.

Suggestion: Consider amending the **Act** to require risk-based OIPC notification where a privacy assessment that involves automated decision making systems identifies a significant risk to privacy of affected individuals (as set out in recommendation 3.4). Notification to the OIPC should be tied to their mandate to assess privacy; if a project involves automated decision systems but does not impact privacy, there should not be a requirement to notify the OIPC.

Recommendation 88 (public bodies required to keep records of decision-making processes of automated decision systems)

Issue:
This recommendation of the Orsborn report would require public bodies to keep records of all automated decision systems.

The purposes of the **Act** relate to both access to information and protection of privacy and should relate to these purposes. This recommendation would go beyond matters that relate to access or privacy.

As an alternative, a provision should be developed which directly relates to documentation that has an impact on privacy. Section 65 of the **Act** sets out a requirement that records be kept for one year where they are used to make a decision about an individual:

> **65.** (1) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

Suggestion: Consider amending section 65 to include a provision stating that where automated decision making affects an individual, records regarding how that decision was made should be kept for at least one year.

Recommendation 89 (OIPC powers to monitor and comment on automated decision systems)

Issue:
Automated decision systems are a specialized area; some of these systems may have an impact on privacy, but some do not. Section 95 of the **Act** provides broad authority to the Commissioner to comment on matters affecting access to information and privacy, which would encompass the use of automated decision systems that involve personal information.

Suggestion: No amendment to the Act required.

---

v) Privacy breach reporting

#	2020 Recommendation (summary)	Notes
90.	That the **Act** be amended to reflect consistency in the requirements to report a privacy breach to the commissioner and to the affected individual and to allow the head of a public body, on notification to the commissioner, to refrain from notifying the individual concerned if there is a risk of significant harm to another person.	Government is supportive of this recommendation.
91.	That all public bodies report privacy breaches to the ATIPP Office as well as to the OIPC.	Government is supportive of this recommendation

vi) Prospective and third party privacy complaints

#	2020 Recommendation (summary)	Notes
92.	Allow complainants to file prospective complaints about privacy breaches.	Government is supportive of this recommendation with modifications.
93.	Remove the requirement for individual consent to the filing of a privacy complaint.	Government is supportive of this recommendation but offers some commentary below for consideration.

Recommendation 92 (prospective privacy breach complaints)

Issue:
Public sector privacy legislation across Canada contains sections setting out the right to make privacy complaints; almost all of these sections focus on concerns about incidents that have happened in the past. They use language such as "a person who believes that the person's own personal information has been collected, used or disclosed in violation of part II may make a privacy complaint" It may be impractical for individuals to make complaints based on possible future decisions of public bodies.

However, Nova Scotia includes legislative authority for investigations by the commissioner into prospective violations of their privacy legislation. Section 103 of Nova Scotia's **Freedom of Information and Protection of Privacy Act** (which is set to come into force in 2027) states that the Commissioner "may, initiate a privacy review if the Commissioner has reasonable grounds to believe that a person has contravened **or is about to contravene** this Part and the subject-matter of the privacy review relates to the contravention."

This would allow the Commissioner to take action on a prospective contravention of the **Act** if there is a strong basis for doing so.

Suggestion: Consider amending the **Act** to allow the OIPC to conduct own motion investigations relating to prospective privacy breaches vs individuals filing complaints. Should the Commissioner use these powers they should exercise discretion and only act where a serious breach is imminent.

Recommendation 93 (privacy complaint and consent)

Issue: Should consent be required for filing a privacy complaint.

The current language in s.73(2) of the **Act** states that:

> (2) Where a person believes on reasonable grounds that personal information has been collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the Commissioner on behalf of an individual or group of individuals, **where that individual or those individuals have given consent to the filing of the privacy complaint**. [emphasis added]

The intention behind this recommendation was to ensure that there is no impediment to the OIPC investigating privacy breaches, as such investigation would be in the public interest.

With the recommended adjustments to recommendation 92 set out above, the issue this recommendation sought to address (the inability to investigate a privacy breach where the individual(s) have not consented to the filing of the complaint) would be resolved. As a result, this recommendation would no longer be required.

Suggestion: Allow the OIPC to conduct own motion investigations relating to privacy complaints and prospective breaches.

---

vii) Anonymity of privacy complaints

#	2020 Recommendation (summary)	Notes
94.	That the **Act** be amended to allow the commissioner to accept a privacy complaint from a person who wishes to remain anonymous, if their identity is not relevant to the investigation.	Government is supportive of this recommendation.

viii) Political parties and personal information

#	2020 Recommendation (summary)	Notes
95.	GNL proceed expeditiously with the development of a regulatory and oversight regime covering the collection, use and	See commentary below.

	disclosure of personal information by registered political parties.	

Recommendation 95 (regulatory oversight regime of political parties and their handling of personal information)

Issue:

Political parties are not regulated by federal privacy legislation. In the provinces and territories, only British Columbia imposes privacy requirements on political parties through their private sector privacy legislation, the **Personal Information Protection Act**; this is not the same act that regulates public bodies in British Columbia.

Political parties are subject to some limited requirements; for example, section 55(4) of the **Elections Act** restricts what the list of electors may be used for. However, political parties are not subject to comprehensive privacy legislation.

While there are legitimate concerns about the collection, use, and disclosure of personal information by political parties, they are not public bodies under the **Act**. Political parties play a different role than public bodies and as such, the regulation and oversight of the collection, use and disclosure of personal information by political parties requires a different approach than that applied to public bodies.

The Office of the Privacy Commissioner of Canada has recommended that political parties be subject to privacy rules similar to those set out in federal legislation, while adapting them to the unique role that political parties play. Political parties play a different role and perform different functions than public bodies; while they should adopt privacy best practices, public sector privacy legislation is not an appropriate venue. This is beyond the scope of the **Act**.

Suggestion: No amendments required to the **Act**.

1.21 Alumni engagement

#	2020 Recommendation (summary)	Notes
96.	Allow post-secondary educational bodies to use personal information in alumni records for outreach and engagement purposes.	Government is supportive of this recommendation.
97.	Allow alumni to request that their personal information cease to be used for outreach and engagement activities.	Government is supportive of this recommendation.

1.22 Complaints, recommendations and appeals

i) Parties to a complaint

#	2020 Recommendation (summary)	Notes
98.	That the **Act** be amended to provide that when a complaint is made regarding information withheld due to third party business interests, the third party is considered a party to the complaint.	Government is supportive of this recommendation.

ii) Complaint investigation process

#	2020 Recommendation (summary)	Notes
99.	That the **Act** be amended to Allow an additional five days for parties to a complaint to make representations to the commissioner and for the initial informal resolution process.	Government is supportive of this recommendation.
100.	Reduce the commissioner's optional extension to the informal resolution process by five days.	Government is supportive of this recommendation.
	Suggestion 5: If a complaint contains insufficient particulars to allow a public body to identify the circumstance in question and respond meaningfully, the OIPC should seek further particulars from the complainant. If no such particulars are forthcoming, the OIPC should consider refusing to investigate the complaint. The OIPC formally advise the complainant and the public body of the cessation of the informal resolution process. The OIPC advise the complainant and the public body no later than five days following the cessation of the informal process of the general conclusions of the OIPC with respect to the complaint and the likely recommendation(s).	Government is supportive of this recommendation.

#	2020 Recommendation (summary)	Notes
	After being so notified, the complainant and the public body be given five days within which to provide the OIPC with a final written submission, should they so choose.	

iii) Extent of the appeal right

#	2020 Recommendation (summary)	Notes
101.	Allow a person to file a complaint for failure to comply with an obligation under the *Act*.	Government is supportive of this recommendation with modification. See commentary below.
102.	Allow the commissioner to make recommendations that a public body take steps to comply with a legal obligation under the *Act* and delete the reference to "failure to act".	See commentary below.
103.	Allow the head of a public body to apply to court for a declaration that the public body is not required to comply with that recommendation.	See commentary below.
104.	Allow the commissioner to file an order with the court directing the head of the public body to take steps to comply with an obligation under the **Act**.	See commentary below.
105.	Allow an applicant or third party to commence an appeal in court of a public body's decision not to take steps to comply with an obligation under the **Act**.	See commentary below.
106.	Allow the court to make an order it considers appropriate should it determine that a public body has not complied with an obligation under the **Act**.	See commentary below.
107.	Remove the option for the commissioner to recommend that a public body reconsider a decision.	Defer to OIPC

Recommendation 101 (filing a complaint for a failure to comply with an obligation under the Act)

Issue:
Currently, the **Act** allows a person to file a complaint respecting a decision, act or failure to act or for correction of personal information. Furthermore, they are able to appeal a "decision, act or failure to act" directly to the Court. However, with regards to their ability to appeal a decision after an OIPC complaint, it is limited to the decision of a public body to grant or refuse access to a record or not make the requested correction of personal information. This was the issue brought forward by both the OIPC and Memorial University during the 2020 ATIPPA Review.

The OIPC has interpreted the legislation broadly in terms of what an applicant can appeal where they first file a complaint, while Memorial University has not. Given section 54 does not include the ability to appeal "an act or failure to act," Memorial argued that an applicant cannot appeal a matter such as the duty to assist, which includes the requirement to conduct a reasonable search. However, the OIPC has argued that an applicant should be able to appeal a decision where they feel a thorough search was not completed. They argue that if a record was not found due to inadequate search, this would be a decision of a public body to refuse access to a record.

In their final report, the 2020 Review Committee recommended that "a failure to act" be replaced with "a legal obligation under the Act," and include it in sections of the **Act** where "a failure to **Act**" does not currently appear. While government supports the intent of this recommendation (to ensure an applicant's right to appeal a decision after the OIPC has issued a report), it is concerned the approach suggested will have unintentional consequences as it modifies provisions throughout the Act to resolve an issue relating to one provision. Therefore, it suggests that the Act be amended to resolve this specific issue by amending section 54 of the Act to include "a failure to Act." This will ensure applicants have the same rights whether they appeal directly to court or appeal after an OIPC complaint.

Suggestion: Consider amending section 54 of the **Act** to include the right to appeal "a failure to act."

Recommendations 102-106 (complying with an obligation under the Act)

Issue:
Recommendations 102-106 of the 2020 ATIPPA Review Committee are subsequent to recommendation 101. As noted above, these recommendations are related to a specific issue of interpretation brought forward by the OIPC and Memorial University during the 2020 ATIPPA Review. If the current Committee were to move forward with the suggestion made by government regarding recommendation 101, there would no longer be a requirement to make the suggested amendments found in recommendations 102-106.

Suggestion: Consider amending section 54 of the **Act** to include the right to appeal "a failure to act." (see rec 101), removing the requirement for these recommendations.

---

iv) Deemed acceptance and the appeal right

#	2020 Recommendation (summary)	Notes
108.	That the **Act** be amended to provide that when the head of a public body has not responded to a recommendation of the commissioner and is thus considered to have complied with it, the commissioner will give written notice of this to the complainant, the public body, and any notified third parties.	Government is supportive of this recommendation.

v) The court process

#	2020 Recommendation (summary)	Notes
109.	That the **Act** be amended to provide that unless otherwise ordered, an appeal shall be subject to case management under Rule 18A.06 and the first step in the proceeding following the filing of the notice of appeal shall be a case management meeting.	See commentary below.

Recommendation 109 (appeals to be subject to case management under Rule 18A.06)

Issue:
Currently it is within the court's purview to decide whether an appeal should go through case management. During the 2020 ATIPPA Review Memorial University suggested that appeals be case managed.

Case management is a process set out by the **Rules Supreme of Court, 1986**. It allows a judge to direct how procedural matters will be addressed and allows those actions to be more organized. The purpose is set out as follows:

> 18A.01. The purpose of this Rule is to provide for selected proceedings a level of management and direction with respect to pre-trial procedures and preparation for trial that is more organized, coordinated and focused than what would be normally applicable to cases proceeding through the system from pleading to trial, with a view to
> (a) ensuring that maximum benefit is gained from each trial day;
> (b) making more efficient use of Court resources;
> (c) ensuring adequate and accurate amounts of time are reserved for trial; and
> (d) providing for the public interest in access to justice in a timely and cost effective manner.

In their 2021 supplemental submission, the OIPC disagreed with this recommendation as they felt it was not necessary in most cases. Government agrees with this position and would note

that making case management a legislative requirement does not appear to be keeping with the intent of 18A.01 of the **Rules Supreme of Court,1986** as outlined above.

Suggestion: No changes are required to the **Act** since the decision of whether to proceed with case management would fall within discretion of the judge presiding over the matter.

---

vi) Application to Supreme Court for a declaration

#	2020 Recommendation (summary)	Notes
110.	That the **Act** be amended to make clear that when a public body seeks a declaration by the court that it is not required to comply with a recommendation of the commissioner, it is by way of an *ex parte* application.	Government is supportive of this recommendation.

1.23 Other issues

i) Whistleblower protection

#	2020 Recommendation (summary)	Notes
	Suggestion 6: That government consider whether or not any public body now subject to **ATIPPA, 2015**, subject to **PIDA**, should by regulation be considered a public body for **PIDA** purposes.	See commentary below.

Suggestion 6 (public interest disclosure and whistleblower protection coverage)

Issue:
This recommendation focused on ensuring that there was coverage for all public bodies subject to the **Act** to be able to make complaints about possible wrongdoing. Based on a review of the public bodies covered by the **Public Interest Disclosure and Whistleblower Protection Act** (**PIDA**) and those subject to the **Act**, the main distinctions would be the exclusion of the following entities from **PIDA** coverage:

- Memorial University
- the House of Assembly and statutory offices
- local public bodies (cities and municipalities)

Memorial University has its own whistleblower policy and process. The House of Assembly and statutory offices are subject to the **House of Assembly Accountability, Integrity and**

Administration Act which includes Part VI relating to public interest disclosure and disclosure of wrongdoing.

Since this suggestion was made in 2021, the **Municipal Conduct Act** came into force (September 2022). This legislation governs conflict of interest, ethical behavior and professional conduct for municipalities. The legislation defines what constitutes a conflict of interest and introduces a common set of rules for all municipalities regarding conflict of interest. The legislation requires municipalities to establish codes of conduct for all municipal officials. It would be worth noting however that regional service boards do not fall under the **Municipal Conduct Act** or **PIDA** but are in fact subject to the **Act**.

Suggestion: No change required to **PIDA** at this time.

---

ii) General amendments

#	2020 Recommendation (summary)	Notes
111.	Make pronouns gender neutral.	Government is supportive of this recommendation.
112.	Update "Trial Division" references to "Supreme Court".	Government is supportive of this recommendation.
113.	Any necessary punctuation and grammar amendments.	Government is supportive of this recommendation.

iii) Other amendments

#	2020 Recommendation (summary)	Notes
114.	Add definition of biometric information to the **ATIPPA, 2015**.	Government is supportive of this recommendation.
115.	Change business day to any day from Monday to Friday but does not include holidays or a. Other days on which a public body is not open for business b. For the purposes of section 42 and 44 other days on which the OIPC is not open for business and c. For the purposes of section 52-54, 54.1, other days on which the Trial Division is not open.	Government is supportive of this recommendation.
116.	That the **Act** be amended to change the definition of personal information:	Government is supportive of this recommendation with modification

#	2020 Recommendation (summary)	Notes
	a. to exclude an individual's business name, address or telephone number b. to add gender c. to add biometric information d. to add IP address if it can be used to identify an individual	specifically to business contact information. See commentary below.
117.	Change to 2x(viii) to specify NL courts (list of public bodies not subject to **ATIPPA, 2015**)	Government is supportive of this recommendation.
118.	Change 5(1)(a) to specify NL courts (list of records excluded from **ATIPPA, 2015**)	Government is supportive of this recommendation.
119.	Change references to Royal Newfoundland Constabulary (RNC) in s.5 to law enforcement	See commentary below.
120.	Changes to 19(7) (third party notification) to note that a public body cannot release records that are part of a third party notification until the time period for filing a complaint or appeal has expired and no copy of the complaint/notice has been provided or they received written notice from the third party that no further recourse will be pursued.	Government is supportive of this recommendation.
121.	Minor changes to s.26(1) and s.26(5) re: fees/costs (estimate and waiver of costs)	See commentary below.
122.	Change to 40(2)(m) (disclosure of attendance/participation at a public event/ receipt of honour/award) – allows disclosure of personal information where not contrary to 40(5) (list of factors to consider when determining if disclosure is an unreasonable invasion of privacy.	See commentary below.
123.	Addition of types of responses an applicant cannot file a complaint with the commissioner for.	Government is supportive of this recommendation.
124.	Change to 49(2) – response from public body to OIPC report	Government is supportive of this recommendation.
125.	Change to 55(d) and (e) – right of appeal to add new subsections. Amend section 55 to	Government is supportive of this recommendation.

#	2020 Recommendation (summary)	Notes
	add "requests that are deemed to be abandoned" and "a decision under paragraph 49(d) to not make an improvement in access"	
126.	Change to 56(6) – procedure on appeal Amend section 56(6) to require that where a third party appeals, the head of the public body should give the applicant notice of the appeal and instructions on how to intervene.	See commentary below.
127.	Change to 66(1)(c) - use of personal information to "or by" a public body	See commentary below.
128.	Change to 68(1)(p) – public body may disclose personal information where there are compelling circumstances that affect a person's health or safety and where disclosure, if appropriate, is given to the individual the information is about.	Government is supportive of this recommendation.
129.	Change to 68(1)(v) – public body may disclose personal information to a surviving spouse where the head of the public body considers it appropriate under the circumstances.	Government is supportive of this recommendation with modification. See commentary below.
130.	Addition of 68(1)(x) – public body may disclose personal information if it is of a type routinely disclosed in a business or professional context and the disclosure is limited to specific information (e.g. name, business contact information, etc.) and does not reveal other personal information about the individual or another person.	See commentary below.
131.	Change to 72(1) – Outlines requirement for department to submit a privacy assessment to the Minister responsible for the **Act**. Amend to state "A Minister shall, during the development of a program or service by a department or branch of government, as defined under subparagraph 2(x)(i), submit to the Minister responsible for the **Act**…	Government is supportive of this recommendation.
132.	Change to 73(4)(a) – one year after the subject matter of the privacy complaint first	Government is supportive of this recommendation.

#	2020 Recommendation (summary)	Notes
	came to the attention of or should reasonably have come to the attention of the complainant or complainants	

Recommendation 116 (definition of personal information)

Issue:
The definition of personal information in the **Act** does not exclude business contact information. Most other public sector privacy legislation explicitly recognizes that business contact information does not have the same sensitivity as name or contact information given in a personal context.

Treating business contact information as personal information can be problematic or impractical in certain circumstances. For example, a public body may need to conduct privacy assessments on projects that only involve business contact information, which from a privacy perspective are very low risk.

OIPC decisions have recognized that business contact information is low sensitivity. See, for example, Department of Fisheries, Forestry and Agriculture (Re), 2021 CanLII 29742 (NL IPC) at paragraphs 8–9.

Here is how various provinces approach this issue:

- Business contact information is excluded from definition of personal information in New Brunswick, Nova Scotia, Ontario, British Columbia, Yukon
- Business contact information is allowed to be disclosed under s. 68 equivalent in PEI, Manitoba, Northwest Territories
- Business contact information is included in the definition of personal information with no clear authority to disclose: Saskatchewan, Nunavut
- Business contact information is included in definition of personal information, except when representing employer: Alberta

Excluding business contact from the definition of personal information may help to clarify the issue as it would apply to both the access to information side of the act and the privacy side. It would also make it clear that privacy assessments are not needed where only business contact information is collected for a project.

However, there may be situations where business contact may be more sensitive, including:

- Some businesses operate from people's homes, making their business address overlap with their personal address. While some small businesses are public-facing

and have their address publicly available, many do not. Some examples include farms and small scale craft producers.

- If the decision is made to address this issue, it should also be recognized that business contact could have more sensitivity if it reveals other personal information. Hypothetically, if government had held a meeting with 'business owners who were struggling with the stress of complying with Covid-19 requirements', notes of that meeting could reveal sensitive information about mental health even though they were provided in a business context.

Suggestion: Amend the definition of personal information under s.2 to exclude business contact information from personal information, unless the information would reveal a person's home address or other personal information about them that is not otherwise publicly available.

Recommendation 119 (change references to the RNC in s.5 to law enforcement)

Issue:
During the 2020 ATIPPA, 2015 Review, Executive Council suggested that provisions of subsection 5(1) of the **Act** that reference the Royal Newfoundland Constabulary ("RNC") extend to equivalent Royal Canadian Mounted Police ("RCMP") records. Specifically:

> 5. (1) This Act applies to all records in the custody of or under the control of a public body but does not apply to
> (k) a record relating to an investigation by the Royal Newfoundland Constabulary if all matters in respect of the investigation have not been completed;
> (l) a record relating to an investigation by the Royal Newfoundland Constabulary that would reveal the identity of a confidential source of information or reveal information provided by that source with respect to a law enforcement matter;
> (m) a record relating to an investigation by the Royal Newfoundland Constabulary in which suspicion of guilt of an identified person is expressed but no charge was ever laid, or relating to prosecutorial consideration of that investigation; or

It is government's position that the RCMP provides comparable services to the RNC within this province, and that the protections afforded to specific RNC records are warranted for the RCMP. These records can involve complex and serious criminal matters. In such situations it is necessary to carefully restrict the number of people who can view these records. The addition of the RCMP is further supported by amendments made to section 5 subsequent to the 2020 review which added comparable provisions for the Serious Incident Response Team (SIRT)-NL (the provincial oversight body for serious incidents involving the RNC and the RCMP).

During the 2020 ATIPPA, 2015 Review, the RNC suggested the broader inclusion of law enforcement to these provisions of the **Act**. Under subsection 2(n) of the **Act**, "law enforcement" is defined as:

> (i) policing, including criminal intelligence operations, or

(ii) investigations, inspections or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead to or could lead to a penalty or sanction being imposed under the enactment;

The relatively broad definition in the legislation, which is primarily relevant to the application of various paragraphs under section 31 of the **Act** (law enforcement), can encompass a wide range of public body activities. For example, it could include municipal, wildlife or environmental enforcement, etc. In various decisions within Canada, this definition has been interpreted to include activities well beyond criminal law matters. For example:

- a violation of municipal zoning bylaws: 2011 CanLII 96582 (AB OIPC) | Edmonton (City) (Re) | CanLII
- a complaint to the veterinary medical association about a veterinarian: 2005 CanLII 4174 (BC IPC) | British Columbia Veterinary Medical Assn., Re | CanLII
- activities around health inspections of restaurants: 2006 CanLII 39088 (PE IPC) | Re Department of Health | CanLII

If the Committee were to agree with this recommendation as proposed, it would result in significantly expanding the scope of this exemption which removes information from the application of the **Act**. Furthermore, it would remove this broader scope of records from OIPC oversight, as per paragraph 97(1)(a) of the **Act** (production of records) which finds that sections 97 and 98 of the **Act** "apply to a record notwithstanding paragraph 5 (1)(c), (d), (e), (f), (g), (h) or (i)."

It is government's position that expanding subsection 5(1) of the **Act** to include "law enforcement" rather than limit it to the RNC and RCMP (and now SIRT) would not be in keeping with the purpose of the **Act** as outlined in section 3. Where there are concerns regarding broader law enforcement records being disclosed, section 31 provides the appropriate level of protection, while ensuring accountability and proper oversight.

Suggestion: Consider modifying this recommendation to only add the RCMP to the relevant paragraphs of subsection 5(1) rather than "law enforcement."

Recommendation 121 (minor changes to s.26(1) and s.26(5) re: fees/costs (estimate and waiver of costs))

Issue:
In the final report for the 2020 ATIPPA Review, the Committee made some drafting suggestions relating to s.26(1) and s.26(5). Given they were minor in nature, no additional information was provided to explain the intent of these. Government is suggesting further review of these drafting recommendations to determine what implications such amendments could have on the **Act**.

Suggestion: Consider further review to determine what implications such amendments may have on the **Act**.

Recommendation 122 (disclosure of attendance or participation at a public event/ receipt of honour/award)

Issue:
Section 40 states that personal information must not be disclosed to an applicant where the disclosure would be an unreasonable invasion of a third party's personal privacy. Subsection 40(2) sets out a variety of categories of personal information that is considered not to be an unreasonable invasion of privacy, including

> (m) the disclosure is not contrary to the public interest as described in subsection (3) and reveals only the following personal information about a third party:
>
> (i) attendance at or participation in a public event or activity related to a public body, including a graduation ceremony, sporting event, cultural program or club, or field trip, or
>
> (ii) receipt of an honour or award granted by or through a public body.

The 2020 review recommended changing the reference in 40(2)(m) from 40(3) to 40(5). S.40(3) explicitly states that "the disclosure of personal information under paragraph (2)(m) is an unreasonable invasion of personal privacy where the third party whom the information is about has requested that the information not be disclosed." Alternatively, s. 40(5) relates to various factors to consider in determining whether disclosure is an unreasonable invasion of privacy and not specifically connected to 40(2)(m).

This recommendation was included in a section suggesting a number of amendments to the **Act**, "primarily for clarification or appropriate updating". There was no discussion of the rationale for the suggested change nor was it raised through any submission made to the committee. As such, it does not appear to be a required amendment.

Suggestion: No change required to s.40(2)(m).

Recommendation 126 (s. 56 - notice of appeal and instructions on how to intervene)

Issue:
Currently, subsection 56(6) of the **Act**, requires "where an appeal is brought by a third party, the head of the public body shall give written notice of the appeal to the applicant." The 2020 Committee recommended amending the **Act** to also require that the head provide instructions on how to intervene.

It is unclear what is intended to be captured by the term "instructions." If "instructions" is meant to include a statement on correspondence advising an applicant that they should contact the Court or file a Notice of Intervention, there would be no concern – government could facilitate this through the development of a standard template. However, if the intent was to provide more substantive instructions there would be concerns that it could appear that a public body was required to provide advice (potentially legal), which would neither be appropriate nor feasible for many smaller public bodies within limited resources.

Suggestion: Consider limiting the scope of this recommendation as noted above.

Recommendation 127 (use of personal information)

Issue:
Section 66(1)(c) of the **Act** states:

> "A public body may use personal information only for a purpose for which that information may be disclosed to that public body under sections 68 to 71."

In the 2020 review, the Orsborn report recommendation 127 suggested that the language be revised to "…for a purpose for which that information may be disclosed **to or** by that public body under sections 68 to 71."

In reviewing the language used by other Canadian jurisdictions, no other province or territory includes "to or by". Those with similar language styles to the **Act** all include only "disclosed to".

Further, it was noted that this was not suggested by stakeholders during the 2020 review process, nor has it been suggested to date in the current review.

It is noted that New Brunswick is the sole variation among legislation with similar language styles – New Brunswick currently uses "disclosed by" rather than "disclosed to".

Suggestion: No amendments are needed to s.66(1)(c).

Recommendation 129 (disclosure to a surviving spouse or relative where head of public body considers it appropriate)

Issue:
The **Act** currently allows disclosure to a surviving spouse or relative of a deceased individual where, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy (s.68(1)(v)).

In the 2020 review, the committee recommended changing this provision to state:

> 68(1)(v) – to the surviving spouse or relative of a deceased individual where the head of the public body considers it appropriate under the circumstances.

This change would allow greater flexibility in certain circumstances to allow the head of a public body to decide to disclose personal information of a deceased individual where they consider it appropriate in the circumstances. This suggested amendment would provide greater flexibility to disclose a deceased individual's personal information, instead of tying it to the "unreasonable invasion of privacy" test that is currently required under this provision.

Ontario's **Freedom of Information and Protection of Privacy Act** ("**FIPPA**") allows disclosure of personal information about a deceased individual to the spouse or a close relative of the deceased individual, and the head is satisfied that, in the circumstances, the disclosure is desirable for compassionate reasons. The difference in these two similar statements lies in the

ability to disclose information for compassionate reasons instead of measuring invasion of privacy.

Suggestion: Amend s.68(1)(v) similar to what was recommended by the 2020 committee; however, also include a provision with language similar to Ontario's s.21(4)(d) of **FIPPA** that would allow the disclosure of personal information to a spouse or close relative of a deceased individual for compassionate reasons.

Recommendation 130 (disclose personal information that is in a business or professional context)

Issue:
The Act does not currently distinguish between personal information and personal information that is generally disclosed in a business or professional context, specifically name, business contact information, etc.

Recommendation 116 suggested that business contact information be removed from the definition of personal information. Therefore, authority to disclose such information would no longer be required under section 68.

Suggestion: Changing the definition of personal information to exclude business contact information as set out in Recommendation 116 would address the issue above.

---

iv) Schedule A

#	2020 Recommendation (summary)	Notes
133.	That section 5.4 of the **Energy Corporation Act** be amended to allow the standard ATIPPA request, review, recommendation and declaration/appeal processes.	Government is supportive of this recommendation but notes that the **Energy Corporation Act** ("**ECA**") has been repealed and replaced by the **Hydro Corporation Act, 2024 ("HCA")**. Section 30 of the **HCA** allows the Minister to request information, records, reports and other documents from the corporation and its subsidiaries.
134.	That **ATIPPA, 2015** be amended to extend the section 9 public interest override provision to section 5.4 of the **Energy Corporation Act**	Government is supportive of this recommendation.
135.	That the **Energy Corporation Act** be amended to limit the application of section	No longer required. See commentary below.

#	2020 Recommendation (summary)	Notes
	5.4 only to hydrocarbon-related information in Nalcor's custody.	
	Suggestion 7: That government consider amending the **Energy Corporation Act** to provide that the corporation is required to provide to the responsible minister such information as may be requested by the minister.	No longer required. See commentary below.
136.	That Schedule A be amended to remove section 8(1) of the **Evidence Act**.	Government is supportive of this recommendation.
137.	That the **Act** be amended to remove section 5(1) of the **Fish Inspection Act** from Schedule A.	Government is supportive of this recommendation in conjunction with recommendation 47.
138.	That the **Act** be amended to remove section 4 of the **Fisheries Act** from Schedule A.	Government is supportive of this recommendation in conjunction with recommendation 47.
139.	That section 21 of the **Innovation and Business Investment Corporation Act** be amended to allow the standard ATIPPA request, review, recommendation and declaration/appeal processes.	Government is supportive of this recommendation.
	Suggestion 8: That government consider an amendment to **ATIPPA, 2015** to extend s. 9 public interest override provision to s. 21 of the **Innovation and Business Investment Corporation Act.**	Government is supportive of this recommendation.
140.	That section 23 of the **Oil and Gas Corporation Act** be amended to allow the standard ATIPPA request, review, recommendation and declaration/appeal processes.	Government is supportive of this recommendation.
	Suggestion 9: That government consider an amendment to **ATIPPA, 2015** to extend the s. 9 public interest override provision to s. 23 of the **Oil and Gas Corporation Act**.	Government is supportive of this recommendation.

#	2020 Recommendation (summary)	Notes
141.	That the **Act** be amended to remove section 18 of the **Workplace Health, Safety and Compensation Act** from Schedule A.	Government is supportive of this recommendation.

Recommendation 135 (limit commercially sensitive information protection under Energy Corporation Act to only hydrocarbon-related information)

Issue:
The **Energy Corporation Act** ("**ECA**") has been repealed and replaced by the **Hydro Corporation Act, 2024** ("**HCA**"). Section 31 of the **HCA** provides protection for commercially sensitive information. The **HCA** defines commercially sensitive information to be: "[…] information of the corporation or a subsidiary, or of a third party provided to the corporation or the subsidiary by the third party, that relates to the exploration for, development, production, refining, marketing and transportation of hydrocarbons and products from hydrocarbons […]".

Suggestion: No changes are required as s.31 of the **HCA** is consistent with the intent of this recommendation.

Suggestion 7

Issue:
The **Energy Corporation Act** was repealed and replaced with the **HCA** which includes section 30 which states - "Where requested by the minister, the corporation or a subsidiary shall provide the minister with the information, records, reports and other documents the minister specifies in the request relating to the business and affairs of the corporation or the subsidiary." As such, this recommendation is no longer required.

Suggestion: No change required.

Part 2 – Access to Information Provisions

Terms of Reference, Mandate Area 2: review exceptions to access, timelines for response, and the effectiveness of current administrative procedures and the current cost schedule.

2.1 Designation and delegation by head of a public body

Issue:
Section 110 of the Act states:

> "The head of a public body shall designate a person on the staff of the public body as the coordinator […]"

The ATIPP Office was centralized under Executive Council in 2024. The intent was to ensure adequate resources dedicated to access to information, privacy, municipal access and privacy support, as well as policy and professional development to support the goal of serving as a centre of excellence in access and privacy.

The ATIPP Office has three divisions, one of which is the Access and Open Information Division. This division employs all ATI and senior ATI coordinators across government. These coordinators are employees of the ATIPP Office; however, those staff are assigned to departments to serve as the coordinator for that department. They function as an employee of their assigned department, reporting to the Executive of that department, in addition to the ATIPP Office.

Given this new structure, as well as situations where smaller public bodies may need to engage a coordinator that is not on the staff of the public body, the current language of s.110 creates a situation where such a designation may not be permitted.

Suggestion: Consider amending section 110 to allow for the designation of a coordinator to be someone other than a member of the staff of the public body.

2.2 Disregard where behaviour of applicant is abusive or malicious

Issue:
Discussions with access coordinators over the past several years have highlighted a concerning shift in some applicant behaviours. There have been situations where an applicant's behaviour has been threatening, intimidating or harassing toward a coordinator. While this is rare in terms of the number of applicants demonstrating these behaviours, it has been noted on a number of occasions over the past 5 years with coordinators having to escalate matters to management or executive intervention and change the method of communicating with the applicant to avoid such behaviours (e.g. email correspondence with the applicant only instead of by phone).

Currently, there is no provision under the **Act** that would allow a public body to ask to disregard a request where an applicant's behaviour would be considered abusive or

malicious. As the employer of coordinators, it is incumbent on public bodies to ensure a safe and respectful workplace, free from harassment or abuse.

This provision is intended to be used only in limited and exceptional situations. It does not allow a public body to unilaterally decide not to respond to a request; rather, the public body must seek the Commissioner's approval and satisfy the Commissioner that the statutory threshold has been met. The onus rests with the public body to provide clear and sufficient evidence demonstrating how the behaviour is abusive and/or malicious. This evidentiary burden, together with independent OIPC oversight and approval, ensures that the provision remains a narrow safeguard and is not used as a routine administrative tool.

British Columbia recently amended its **Freedom of Information and Protection of Privacy Act** to specifically account for these rare but serious circumstances to ensure that employees are protected.

> **43** If the head of a public body asks, the commissioner may authorize the public body to disregard a request under section 5 or 29, including because
> […]
> (a.1) the behaviour of the applicant is abusive or malicious,
> […]

British Columbia's Information and Privacy Commissioner has recently issued guidance on application to disregard requests under this new provision, including definitions and examples of the terms "abusive" and "malicious".

Specifically, the Commissioner defines "abusive" as:

> "a pattern of behaviour that is offensive, mistreats others, or involves threats, insults, put downs, criticism, intimidation, or humiliation."

"Malicious" is defined as:

> "intentional conduct undertaken without just cause or excuse, particularly where the action is motivated by an improper purpose, ill will, or mischievous intentions or motives. This generally means actions intended to cause pain or cost a public body resources or time […]"

In Newfoundland and Labrador, the Office of the Information and Privacy Commissioner has recently published its Unreasonable Behaviour Policy that also addresses the expectation of the behaviour of individuals with staff of the OIPC. It specifies that behaviour may be considered unreasonable when it falls into one of several categories including "disrespectful, aggressive, or threatening interactions that is:

- is abusive, derogatory, discriminatory;
- uses threatening language;
- involves name calling or insults;
- consists of shouting, interrupting or incessant speech;
- attempts to pressure or intimidate;

- attempts to control access to any one staff member;
- uses high volume communication that disrupts or interferes with office processes; or
- uses public escalation to attempt to influence or interfere with investigations.

The policy goes on to set out an escalation process where such behaviour is exhibited which includes things like limiting communication methods, having a single point of contact, ending conversations and not reviewing or responding to communications.

One of the areas that can lead to uncertainty with coordinators is the legislated duty to assist and the requirement to respond to an applicant. There is no legislative mechanism that currently exists to allow for a public body to not respond to an applicant due to abusive or malicious behavior. Section 21 as it currently exists considers only the request itself – not the behaviour of an applicant.

Suggestion: Amend section 21 of the **Act** to include a provision similar to British Columbia's section 43(a.1) to allow for a public body to apply to the commissioner for approval to disregard a request where the behaviour of the applicant is abusive or malicious.

2.3 Managing records provided to the Commissioner by a public body

Issue:
Public bodies regularly provide records to the OIPC for consideration of a matter during complaint, investigation, audit or privacy assessment processes. This often includes confidential and sensitive information. The provision of this information is critical to enable the commissioner to carry out their duties under the **Act**.

Given the obligations on public bodies to ensure the appropriate handling and protection of public body information and records, it would appear prudent to ensure that records/information provided to the commissioner during a complaint, investigation, audit or privacy assessment process are returned or disposed of appropriately upon conclusion of the matter.

Alberta and Ontario have provisions written in their respective access and privacy laws regarding the handling of records by the commissioner.

Alberta's **Access to Information Act**, s.50(5) states:

> 50(5) After completing a review or investigation, the Commissioner must
> (a) return any original paper record produced to the Commissioner, and
> (b) destroy any copy of any record, including any electronic record, produced to the Commissioner.

Ontario's **Freedom of Information and Protection of Privacy Act**, s.52(5) states:

> 52 (5) The Commissioner shall not retain any information obtained from a record under subsection (4).

Suggestion: Consider adding a requirement under Part II, Division 3 to require the commissioner to return or securely destroy any records provided to them after completing an investigation. Consider whether to extend this requirement to records provided through an audit process or through a privacy assessment process.

2.4 Section 12 – applicant anonymity

Issue:
Subsection 12(1) of the **Act** requires that the identity and type of applicant remain anonymous while processing a request. Subsection (2) outlines the circumstances under which subsection (1) does not apply. This includes paragraph 12(2)(b) which states that subsection (1) does not apply "where the name of the applicant is necessary to respond to the request and the applicant has consented to its disclosure."

The requirement to have the applicant consent is not practical in the instances where there would be a legitimate need to provide this information to someone other than the coordinator or coordinator's assistant during the processing of a request. For example, in some cases an applicant may make a general request and the responsive records include correspondence to/from them, which often includes personal information that would be withheld under subsection 40(1) if any other applicant had made the request. Without providing the name of the applicant to the head of the public body when they review the final response, it is unclear why the coordinator is suggesting the disclosure of such information. The head may identify this information and ask the coordinator why it is being released. Based on paragraph 12(2)(b), the coordinator would not be able to advise the head of the public body of this without first contacting the applicant and asking for their consent even though this information is required in order for the head of the public body to make the final decision regarding the response to the applicant.

Three other jurisdictions have comparable anonymity provisions in their legislation (Yukon, Northwest Territories and Nunavut). Nunavut's legislation has similar exceptions to **ATIPPA, 2015**, while Yukon and Northwest Territories have provisions that would capture instances where sharing information is required as outlined above:

- Paragraph 45(2)(ii) of Yukon's **Access to Information and Protection of Privacy Act** - "the disclosure is necessary for the head of the responsive public body to respond to the access request,"
- Subsection 6(4) of the Northwest Territories' **Access to Information and Protection of Privacy Act** – "The identity of an applicant shall be kept confidential by the head of the public body and the coordinator designated under section 68.1, and may be disclosed only to the extent required to respond to the request for access."

Yukon's section on anonymity is similar in structure to Newfoundland and Labrador's s.12 – it outlines what information cannot be shared and under what circumstances it can be, whereas the Northwest Territories legislation is less prescriptive.

Suggestion: Consider amending subsection 12(2) to provide additional authority to disclose the identity where it is necessary for the head of the responsive public body to respond to the access request, similar to Yukon's legislation.

2.5 Non-responsive information

Issue:
Requests are generally made in relation to specific information/subjects. However, responsive records often include information unrelated to the request (i.e. non-responsive). For example, meeting notes, agendas or emails may contain information relating to the subject matter of the request, but also contain information relating to other, non-responsive information. The OIPC has issued a practice bulletin-Redacting Non-Responsive Information in a Responsive Document outlining under what circumstances information can be removed as non-responsive. While public bodies are able to remove non-responsive information in limited circumstances, the process outlined in the OIPC guidance document is time consuming and creates additional administrative effort given the information in question is unrelated to an applicant's request.

In Stevens v. Nova Scotia (Labour), 2012 NSSC 367 (CanLII), the judge discusses the issue of non-responsive information (referred to as non-applicable) within the decision. While both non-applicable documents and non-applicable information contained within documents were discussed, the following is in reference to both:

> It appears the initial review officer may have taken the position that the Respondent could not withhold documents on the basis that they were irrelevant. The Respondent referred to those materials as "not applicable". According to the Respondent the Review Officer suggested there was no recognized exemption under FOIPOP legislation for "non applicable" materials. Any such ruling would defy common sense. What possible relevance would it be to the Appellant if someone commented in a document that their grandmother had a wart removed from her nose. (Not that any such comment was made in the redacted materials). With e-mail communications the author on a number of occasions mixed personal or non relevant communications with information which was properly disclosed. The personal, non relevant, information is not something to which the Appellant is entitled to access. There are some things in records, such as e-mail, which are clearly irrelevant and should not be disclosed.

Subsection 16(1.1) of New Brunswick's **Right to Information and Protection of Privacy Act** allows the head of a public body to remove information contained within a responsive record "if, in the opinion of the head, the information is not relevant to the request for information."

Given the finite resources available for processing access to information requests, it seems unnecessary to require public bodies to review and process information contained within a record unrelated to the applicant's request. Having to process information contained in a record that is not responsive to the request also results in additional time being needed to process those portions which are not responsive to the request, thereby impacting the timely access to information by an applicant. In addition to requiring additional time, it can be misleading if exceptions to disclosure are applied to non-responsive information, as it appears that the public body is withholding information related to the request, when in fact they are removing information unrelated to the request.

Suggestion: Consider amending section 8 of the **Act** to allow for non-responsive information within a responsive record to be withheld from disclosure as non-responsive.

2.6 Definition of records and exclusion of back-up systems

Issue:
The Office of the Chief Information Officer currently maintains back-up systems of government data for disaster recovery purposes. There may be other public bodies outside of core government that do the same.

These back-up systems are designed solely for the purpose of recovery in the event of a disaster for business continuity purposes. They are not designed to support routine recovery of data and would require extraordinary effort to search in the event of an access to information request. Further to this, records that have been appropriately destroyed in accordance with the **Management of Information Act** (for those public bodies subject to **MOIA**) and any related retention schedules have been properly deleted and should not be recovered in response to an access request where that information is only maintained for disaster recovery purposes. It is impractical and inappropriate to process requests for these records.

Suggestion: Add "back-up recovery systems" to section 5 of the **Act**; this would exclude records that are only maintained for backup disaster recovery purposes and are not set up to search.

2.7 Jurisdiction of the OIPC related to specific s.5 records

Issue:
Authority of OIPC to investigate complaints for which they do not have the authority to compel production of records.

Section 97 of the **Act** appears to create a two-tiered approach as it relates to s.5 records. Specifically, s.97(1)(a) gives the OIPC the power to compel production of certain classes of s.5 records (e.g. personal or constituency records of an MHA; records of a registered political party or caucus; personal or constituency records of a minister; etc.).

Conversely, there are several classes of s.5 records for which the OIPC does not have the authority to compel their production (paragraph 5(1)(a), (b), (j), (k), (k.1), (l), (m), or (n); e.g. records in a court file; notes, communications or draft decision of a person acting in a judicial or quasi-judicial capacity; ongoing prosecution records; ongoing RNC investigation records; records related to an investigation by the RNC in which suspicion of guilt of an identified person is expressed but no charge was ever laid, etc.).

The question has been raised in a number of instances in the past several years regarding whether the OIPC has jurisdiction to consider a complaint raised related to records identified under paragraph 5(1)(a), (b), (j), (k), (k.1), (l), (m), or (n).

> (a) a record in a court file, a record of a judge of the Court of Appeal, Trial Division, or Provincial Court, a judicial administration record or a record relating to support services provided to the judges of those courts;
>
> (b) a note, communication or draft decision of a person acting in a judicial or quasi-judicial capacity;
>
> (j) a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed;
>
> (k) a record relating to an investigation by the Royal Newfoundland Constabulary if all matters in respect of the investigation have not been completed;
>
> (k.1) a record relating to an investigation by the Serious Incident Response Team as defined under the **Serious Incident Response Team Act** if all matters in respect of the investigation have not been completed
>
> (l) a record relating to an investigation by the Royal Newfoundland Constabulary that would reveal the identity of a confidential source of information or reveal information provided by that source with respect to a law enforcement matter;
>
> (m) a record relating to an investigation by the Royal Newfoundland Constabulary in which suspicion of guilt of an identified person is expressed but no charge was ever laid, or relating to prosecutorial consideration of that investigation; or
>
> (n) a record relating to an investigation by the Serious Incident Response Team as defined under the **Serious Incident Response Team Act** in which suspicion of guilt of a police officer is expressed but no charge was ever laid, or relating to prosecutorial consideration of that investigation.

Suggestion: Clarify whether the OIPC has authority to receive and investigate complaints related to those s.5 records where they do not have authority to compel production of those records.

2.8 Public prosecution files

Issue:
Public Prosecutions occupies a unique role within government. Prosecutors are entrusted with making independent decisions regarding criminal proceedings based on established legal principles, including whether there is a reasonable prospect of conviction and whether a prosecution is in the public interest. The administration of justice depends on prosecutors being able to make these decisions free from actual or perceived external influence, regardless of whether those decisions may be difficult, controversial, or unpopular.

The Supreme Court of Canada in R. v. Anderson, 2014 SCC 41, described prosecutorial discretion and its importance to our system of justice at paragraphs 37, 44, 46, and 47 respectively as follows:

> This Court has repeatedly affirmed that prosecutorial discretion is a necessary part of a properly functioning criminal justice system: *Beare*, at p. 410; *R. v. T. (V.)*, [1992] 1 S.C.R. 749, at pp. 758-62; *R. v. Cook*, [1997] 1 S.C.R. 1113, at para. 19. In *Miazga v. Kvello Estate*, 2009 SCC 51, [2009] 3 S.C.R. 339, at para. 47, the fundamental importance of prosecutorial discretion was said to lie, "not in protecting the interests of individual Crown attorneys, but in advancing the public interest by enabling prosecutors to make discretionary decisions in fulfilment of their professional obligations without fear of judicial or political interference, thus fulfilling their *quasi*-judicial role as 'ministers of justice'". More recently, in *Sriskandarajah v. United States of America*, 2012 SCC 70, [2012] 3 S.C.R. 609, at para. 27, this Court observed that "[n]ot only does prosecutorial discretion accord with the principles of fundamental justice — it constitutes an indispensable device for the effective enforcement of the criminal law".
>
> […]
>
> In an effort to clarify, I think we should start by recognizing that the term "prosecutorial discretion" is an expansive term that covers all "decisions regarding the nature and extent of the prosecution and the Attorney General's participation in it" (*Krieger*, at para. 47). As this Court has repeatedly noted, "[p]rosecutorial discretion refers to the discretion exercised by the Attorney-General in matters within his authority in relation to the prosecution of criminal offences" (*Krieger*, at para. 44, citing *Power*, at p. 622, quoting D. Vanek, "Prosecutorial Discretion" (1988), 30 *Crim. L.Q.* 219, at p. 219 (emphasis added)). While it is likely impossible to create an exhaustive list of the decisions that fall within the nature and extent of a prosecution, further examples to those in *Krieger* include: the decision to repudiate a plea agreement (as in *R. v. Nixon*, 2011 SCC 34, [2011] 2 S.C.R. 566); the decision to pursue a dangerous offender application; the decision to prefer a direct indictment; the decision to charge multiple offences; the decision to negotiate a plea; the decision to proceed summarily or by indictment; and the decision to initiate an appeal. All pertain to the nature and extent of the prosecution. As can be seen, many stem from the provisions of the *Code* itself, including the decision in this case to tender the Notice.
>
> […]

The many decisions that Crown prosecutors are called upon to make in the exercise of their prosecutorial discretion must not be subjected to routine second-guessing by the courts. The courts have long recognized that decisions involving prosecutorial discretion are unlike other decisions made by the executive: see M, Code, "Judicial Review of Prosecutorial Decisions: A Short History of Costs and Benefits, in Response to Justice Rosenberg" (2009), 34 Queen's L.J. 863, at p. 867. Judicial non-interference with prosecutorial discretion has been referred to as a "matter of principle based on the doctrine of separation of powers as well as a matter of policy founded on the efficiency of the system of criminal justice" which also recognizes that prosecutorial discretion is "especially ill-suited to judicial review": Power, at p. 623. In Krieger, the Court discussed the separation of powers doctrine as a basis for judicial deference to prosecutorial discretion:

> In our theory of government, it is the sovereign who holds the power to prosecute his or her subjects. A decision of the Attorney General, or of his or her agents, within the authority delegated to him or her by the sovereign is not subject to interference by other arms of

> government. An exercise of prosecutorial discretion will, therefore, be treated with deference by the courts and by other members of the executive […] [para. 45]

The Court also noted the more practical problems associated with regular review of prosecutorial discretion:

> The quasi-judicial function of the Attorney General cannot be subjected to interference from parties who are not as competent to consider the various factors involved in making a decision to prosecute. To subject such decisions to political interference, or to judicial supervision, could erode the integrity of our system of prosecution. [para. 32]

As prosecutorial independence is necessary to ensure that Crown attorneys can exercise prosecutorial discretion free from political interference, many processes are in place to establish Public Prosecutions independence from the Department of Justice and Public Safety and government generally. Public Prosecutions' files are not accessible by anyone other than employees of the Division, not even the Attorney General. The Attorney General does not have direct oversight of the day-to-day operations of Public Prosecutions; in fact it would be improper for the Attorney General to direct the prosecution of any matter. Instead, Public Prosecutions is delegated the prosecutorial authority from the Attorney General by well settled common law and as particularized by the Public Prosecutions Guidebook.

Currently paragraph 5(1)(j) of the **Act** excludes records relating to a prosecution "if all proceedings in respect of the prosecution have not been completed." Government questions distinguishing between active and concluded prosecution files given many of the underlying concerns outlined below persist after a prosecution has been concluded. Even when a prosecution is concluded there can be an interest in not providing records as proceedings could be re-instituted or related charges could be contemplated. Evidence contained within the file requested, if provided under ATIPPA, could allow the tailoring of further evidence/statements which would interfere with the related investigation and prosecution and negatively impact the reliability of both sets of evidence/statements.

Prosecution files routinely contain solicitor-client privileged information, litigation privileged information, law enforcement information, witness and victim information, confidential source information, and prosecutorial work product. While existing exemptions may protect much of this information from disclosure, it is the experience of Public Prosecutions that concerns may not be fully addressed through severing and redaction. Prosecution files are highly contextual records, and details regarding events, locations, relationships, timelines, or investigative steps may permit the identification of victims, witnesses, or confidential sources even where direct identifiers have been removed – commonly known as the mosaic effect.

In British Columbia's OIPC Order F26-03, the adjudicator describes the mosaic effect:

> The mosaic effect refers to circumstances where seemingly innocuous information can be linked with other available information and used to identify individuals, thereby transforming the innocuous information into personal information.

However, as British Columbia Order F21-47 finds, in the context of an access to information request, when "invoking the "mosaic effect" a public body must explain the logic that leads to

the conclusion that it is reasonable to expect that it might apply. Mere speculation is insufficient to establish its application in a particular case."

As noted above, even when redactions are made that appear reasonable, given the amount of information that may already be in the public domain given open court principles, it is possible that someone with knowledge of events or the ability to access various sources of information through the courts could re-identify redacted information – however, it may be difficult to meet the burden under an access to information request.

While on its face, redactions appear to have appropriately protected information which would be an unreasonable invasion of privacy or of a safety concern, there is potential that those familiar with the cases (whether it be the accused, other witnesses, sources, etc.) could infer details based on what remains. It can be very simple for a motivated individual to fill in information gaps with other information they have been able to gather from other sources. As a result, the risk extends beyond the disclosure of individual pieces of information to the cumulative effect of information contained throughout the record. For example, it is not uncommon for those charged with crimes related to drugs and firearms trafficking to pool and share information from their disclosure packages in an attempt to piece together information that has been redacted to protect the identity of confidential informants in order to determine exactly that information. If in that scenario they then make an ATI request, the person vetting those concluded files may inadvertently provide a piece of information that then exposes the identity of a confidential informant whose safety would then be at great risk.

Government recognizes the importance of openness and transparency as it relates to the Act – it is guided by these principles in each matter it prosecutes, which are subject to established disclosure processes within the criminal justice system. Accused persons are entitled to extensive disclosure in accordance with constitutional and legal requirements, and disputes regarding disclosure are ultimately resolved through judicial oversight. Other records may also be publicly available through the Courts or through access to information requests to police agencies.

As noted above, Prosecution files can contain various types of records, including police files, files of other investigative agencies including audio and video recordings of statements, videos of premises including private dwellings depicting unrelated individuals (including children), body worn camera footage from enforcement and police officers that could depict any number of individuals, photos of places, vehicles and people (alive and deceased, including child exploitation materials), child protection records, court decisions, criminal records, court orders, docket information, internal legal research, internal information sharing documents for oversight and decision making, and information recorded by prosecutors to comply with their duty to document their use of prosecutorial discretion.

Much of this material is highly trauma inducing and should not be reviewed by anyone other than those who must, for a legitimate criminal justice purpose, even then, with sufficient wellness supports in place. Investigative agencies in the province are already subject to ATIPPA regimes and they are in the best position to determine what should be vetted from their files. These agencies, including police agencies, know what other investigations they are conducting and are more aware of the safety and intelligence concerns that could be

impacted by the disclosure of information in their files. Similarly, child protection information is more properly sought from the agency that created the record.

Court decisions, criminal records, court orders and docket information are all created by the Court of Appeal, Supreme Court of Newfoundland and Labrador, and the Provincial Court of Newfoundland and Labrador. All of these documents are readily available from the court that created it.

Public Prosecutions employees create such records as internal legal research, internal information sharing documents for oversight and decision making, and information recorded by prosecutors to comply with their duty to document their use of prosecutorial discretion. They may also have communications with the investigative agencies, expert witnesses, and defence counsel. Most of these would be protected under solicitor-client privilege, legal advice or prosecutorial discretion.

This matter has been contemplated in other jurisdictions. Subsection 4(b) of New Brunswick's **Right to Information and Protection of Privacy Act** excludes "a record pertaining to legal affairs that relate to the performance of the duties and functions of the Office of the Attorney General." Subsection 5 (n) of Alberta's **Access to Information Act** excludes "a record, including any charging recommendation, created by or on behalf of or that is in the custody or under the control of a prosecutor relating to a prosecution or potential prosecution." In reviewing, Alberta's language more closely captures the concerns relating to prosecution files – its exemption is narrow in scope and would not extend to all records under the custody or control of Public Prosecutions (e.g. budget information, government briefing materials, etc.), nor would it extend to the Civil Division (which would also fall under the Office of the Attorney General).

While most other jurisdictions have exemptions equivalent to the **Act**'s s.5(1)(i), many have broad legal privilege provisions that capture prosecution files, which are not contained within the **Act** (e.g. Prince Edward Island, Manitoba, Yukon, Northwest Territories). In subsection 27(1) of Manitoba's **Freedom of Information and Protection of Privacy Act**, the head of a public body may refuse to disclose:

> (b) information prepared by or for an agent or lawyer of the Minister of Justice and Attorney-General or the public body in relation to a matter involving the provision of legal advice or legal services or in relation to the investigation or prosecution of an offence; or
>
> (c) information in correspondence between an agent or lawyer of the Minister of Justice and Attorney-General or the public body and any other person in relation to a matter involving the provision of legal advice or legal services or in relation to the investigation or prosecution of an offence.

Unlike Alberta's **Access to Information** subsection 5(n), these provisions are quite broad and would expand the privilege under s.30 significantly, capturing records other than prosecution files which are being contemplated here.

Given these considerations, it is important to consider whether prosecution records should continue to be addressed primarily through exemptions to disclosure or whether broader exclusion from the **Act** should apply, similar to records in a court file (paragraph 5(1)(a) of the

Act). Expanding the existing exclusion in paragraph 5(1)(j) or otherwise excluding prosecution records from the application of the **Act** would recognize the unique role and independence of prosecutors, better protect sensitive criminal justice information, preserve public confidence in the administration of justice, and acknowledge that prosecution records are already governed by established disclosure and oversight processes within the criminal justice system. While transparency and accountability remain important objectives, prosecutorial decision-making is already subject to judicial oversight and public scrutiny through the courts. Access to prosecution records is also governed through established disclosure and evidentiary processes within the criminal justice system. The issue, therefore, is not whether prosecutorial decisions should be subject to scrutiny through access to information, but whether the Act is the appropriate mechanism for accessing records created in the exercise of Public Prosecutions' independent prosecutorial function.

Suggestion: If the Committee determines that excluding prosecution records from the Act is appropriate, it is suggested either amending s.5(1)(j) or adopting language similar to Alberta's legislation.

Alternatively, if the Committee determines that records currently subject to the **Act** should remain, government would suggest considering:

1. **Expanding the scope of legal privilege -** If this is considered, it would be important to review the scope of any new provision to ensure it wouldn't inadvertently expand the privilege beyond what is being proposed here.

2. **Allow Public Prosecutions to exclude police investigation records from ATI requests submitted -** These records are more appropriately accessed through police organizations that fall under this **Act** or comparable legislation.

Part 3 – Privacy Safeguards and Emerging Technologies

Terms of Reference, Mandate Area 3: evaluate whether ATIPPA, 2015 adequately addresses risks associated with newly evolving technologies, including artificial intelligence, biometric data, and surveillance technologies.

3.1 Privacy notice content

Issue:
Privacy notice requirements across Canada are generally consistent and based on three core elements: notifying individuals of the purpose for collecting their personal information, the legal authority for the collection, and a contact person who can answer questions. Most jurisdictions, including New Brunswick, Prince Edward Island, Ontario, Manitoba, British Columbia, Yukon, Nunavut, and the Northwest Territories, require these basic components when personal information is collected directly from an individual.

Two provinces have notable differences to notice requirements:

- Quebec - Section 65 of **A-2.1** - **Act respecting Access to documents held by public bodies and the Protection of personal information** contains the standard requirements for notice, but also adds:
  - whether providing information is mandatory or optional,
  - the consequences of refusing to provide information,
  - individuals' access and correction rights, and,
  - where applicable, disclosures to third parties or transfers outside the province.

- Alberta – Section 5(2) of **Protection of Privacy Act** contains the standard requirements for notice, but adds:
  - Any intention by the public body to input the information into an automated system to generate content or make decisions, recommendations or predictions

Government has established an AI policy which outlines the guiding principles in the responsible use of AI. These principles include a requirement to be transparent in its use of AI and to explain how information is used and how decisions are made affecting them:

> Transparent and Explainable: People are informed about when and how automation is used and are provided with meaningful information about decisions affecting them.

Including a requirement under s.62(2) (privacy notice requirements) to notify individuals where an automated decision system is being used to make a decision about them would codify this policy in legislation. This is also consistent with the privacy principles which underpin the **Act**, specifically the openness principle which is defined by the Organisation for Economic Co-operation and Development (OECD) as:

> **Openness Principle**
> 12.There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing

> the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Where a public body uses an automated decision system to make or assist with a decision about an individual, the privacy notice should clearly identify that use. This additional notice requirement supports transparency and procedural fairness by helping individuals understand when technology may influence a decision affecting them, what personal information may be used, and how they may seek further information or recourse. It also promotes public trust and accountability by ensuring that the use of automated decision systems is visible to individuals at the point where their personal information is collected, used, or relied upon.

Suggestion: Consider retaining the current requirements to notify individuals of the purpose for collecting their personal information, the legal authority for the collection, and a contact person who can answer questions; however, consider adding the following requirements:

- Clarity on whether the collection is optional or mandatory and any consequences of not providing personal information
- Whether automated decision systems will be used to generate content about the individual or make decisions, recommendations or predictions.

3.2 Making the Act flexible as technology evolves

Issue:
In recent years, the pace of technological change has increased rapidly, affecting how we collect personal information, how we use it and how we protect it. Technological change has also led to an increased risk of cybersecurity incidents.

It can be difficult to legislate for technological change; legislative change moves relatively slowly, while it can be difficult to predict what developments will occur in the next five or 10 years.

A more flexible approach would be to keep the core principles in the Act while placing specific and technical requirements, particularly those under Part III, in regulation or policy. This would allow standards to be updated more quickly in response to technological change, while still preserving the stability and authority of the Act's main privacy protections.

This approach has been taken with Newfoundland and Labrador's Public Procurement framework which sets out requirements in the Act, with the details of how those requirements are to be achieved being set out in Regulations and in policy.

There are a number of suggested additions to the **Act** regarding privacy requirements, including:

- The designation of someone responsible for privacy obligations (privacy officer), and
- Considerations for location of storage of personal data

With respect to guidelines around Privacy Impact Assessments, some provinces set out requirements for the content of Privacy Assessments in regulations. If such regulations are developed, this will also be a good opportunity to incorporate a concept of proportionality.

Suggestion: Amend section 116 to include provisions allowing for:

- Setting standards for reasonable security
- Setting standards for the content of Privacy Impact Assessments and Preliminary Privacy Impact Assessments, including the concept of proportionality.
- Defining "automated decision making" and 'algorithmic impact assessment"
- Setting Standards for the content of Algorithmic Impact Assessments
- Setting standards for Information Sharing Agreements
- Setting standards for safeguarding personal information
- Clarifying the definition of "risk of significant harm"
- Content of privacy notices
- Storing personal information outside of Canada and setting out exceptions for Canadian data residency requirements of personal information (per Issue 4.4 – Data Residency)
- Requirements when sharing personal information for common programs and services
- Clarifying who may act for a minor, a deceased person or an adult
- Defining a word or phrase not defined in this Act

3.3 Proportionality in privacy assessments

Issue:
Currently, the **Act** does not specifically consider proportionality in relation to privacy assessments (including both preliminary privacy impact assessments and privacy impact assessments).

Across Canada, many jurisdictions do not address proportionality, but those that do address it are referring to it in a more general way, in that the direction is to weigh the benefits of the project against the risks to privacy. Several have further direction in policy on what questions to ask to determine the risk to privacy and the benefits of the program.

Quebec is the only jurisdiction with specific legislative reference – s.63.5 of their Act states that "the conduct of a privacy impact assessment under this Act must be proportionate to the sensitivity of the information concerned, the purposes for which it is to be used, the quantity and distribution of the information and the medium on which it is stored."

With proportionality considered in the development of privacy assessments, it would be ensuring that appropriate focus is put in the right areas.

In a 2021 letter to the Senate, the Privacy Commissioner of Canada discussed necessity and proportionality:

> Necessity and proportionality means that organizations should only pursue privacy invasive activities where it is demonstrated that they are necessary to achieve a

> pressing and substantial purpose and where the intrusion is proportional to the benefits to be gained.

Suggestion: It is suggested that the review consider including proportionality as a factor in the completion of privacy assessments.

3.4 Notifying the OIPC of privacy assessments

Issue:
Currently, privacy impact assessments must be provided to the Commissioner where the initiative involves a common or integrated program or service. Specifically, s.72(4) states:

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

The Commissioner may also ask for any privacy impact assessments as part of their general mandate to review compliance with the Act, and these are provided by public bodies on a regular basis.

Commissioner oversight is important. However, it is recommended that the trigger for this oversight should be based on risk, not the type of program or service that is being considered. The purpose of notifying the OIPC at an early stage is not to make the Commissioner responsible for approving privacy assessments, but to ensure timely awareness of initiatives that may present significant privacy risks. Early notification allows the OIPC to identify issues or provide guidance while the public body is still in a position to address privacy concerns before implementation.

Any notification requirement should be risk-based and proportionate. It should apply to privacy assessments involving high-risk initiatives, such as digital identity services, large-scale information sharing, sensitive personal information, or initiatives involving vulnerable populations.

Public bodies would remain responsible for completing privacy assessments, identifying and mitigating risks, and making implementation decisions. OIPC notification would support oversight and guidance but would not replace the public body's accountability for compliance with the Act.

Under Article 36 of the European Union's **General Data Protection Regulation** (**GDPR**), consultation with the supervisory authority is required where processing would result in a high risk:

> Article 36
> 1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing

would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Suggestion: Amend the requirements for privacy assessment review by the Commissioner to remove the requirement for consultation with the OIPC on common or integrated programs or services and replace with a mandatory consultation on programs or services where there is a high risk identified.

3.5 Inferred personal information

Issue:
Public bodies may make inferences about individuals through manual reviews, professional assessments, program eligibility decisions, risk scoring, investigations, audits, data matching, statistical analysis, or policy and service delivery processes. AI systems also have the ability to create or infer personal information about individuals, but inferences about individuals are not limited to AI. Any information inferred about an identifiable individual, whether created by AI, another automated tool, or a person applying judgment to available information, should clearly be identified as personal information.

The Government of Canada recently introduced Bill C-36, intended to replace Part 1 of the **Personal Information Protection and Electronic Documents Act**. This Bill would create the **Protecting Privacy and Consumer Data Act (PPCDA)**.

Bill C-36 defines personal information as "information about an identifiable individual, including information that is inferred about the individual".

Inferred personal information is information that is not directly provided by an individual, but is created by drawing conclusions from other information about them. These conclusions may be made by an AI system, another automated or analytical tool, or by a person reviewing records and applying judgment or expertise. For example, information may be inferred from a person's location history, online activity, service usage, application details, case notes, income information, education or employment history, health information, family circumstances, complaints, investigation records, or interactions with a public body. Inferences may include conclusions, predictions, assessments, scores, flags, categories, opinions, or assumptions about a person's interests, habits, needs, vulnerability, health status, financial situation, reliability, eligibility, compliance, risk level, or likelihood of a future outcome. Even if the inference is uncertain, preliminary, or based on incomplete information, it can still be personal information if it relates to an identifiable individual.

Inferred personal information can create significant privacy risks because individuals may not know that the information exists, may not understand how it was created, and may have limited ability to challenge or correct it. Inferences may also be inaccurate, incomplete, or based on information collected for another purpose. If inferred information is used to make or support decisions about a person, it may affect access to services, benefits, employment, investigations, or other important outcomes. For these reasons, inferred information should be treated with the same care as other personal information, including clear authority for its collection, use and disclosure, appropriate transparency, accuracy checks, safeguards,

retention limits, and human oversight where it may affect an individual's rights, interests, or opportunities.

Suggestion: Add "including information that is inferred about the individual" to the definition of personal information.

Part 4 – Personal Information Protection

Terms of Reference, Mandate Area 4: examine whether current definitions and protections for personal information are sufficient given evolving data collection practices; consider enhanced safeguards for sensitive categories of data; consider whether clarification is needed around minors' rights to access or protect their personal information.

4.1 Define "sensitive personal information"

Issue:
There is currently no definition for "sensitive personal information". The absence of a definition may make it difficult to identify information that should be treated with a higher level of care/protection due to the nature of its content. Disclosure of sensitive personal information could also result in significant harm to an individual.

The concept of a spectrum of sensitivity of personal information is also currently being considered in the federal review of the Privacy Act. Under Theme 3 of the Treasury Board Secretariat's **2026 Review of the Privacy Act: Policy Approaches** document, it states:

> The current *Privacy Act* applies the same level of protection to all personal data, no matter how sensitive it is. This one-size-fits-all approach does not highlight when greater safeguards are required for highly sensitive data, or when fewer safeguards might be appropriate because protections are already applied to the data.
>
> A modernized *Privacy Act* would apply safeguards based on the sensitivity of the data. This would help federal institutions better protect privacy while they deliver programs and services to Canadians. It would also support a more balanced approach to privacy, where protections are practical, focused on real risks, and better matched to the type of data being handled.

A review of other Canadian jurisdictions reveal that currently only Quebec includes a definition of what is sensitive personal information in legislation. In s.59 of Quebec's **Act respecting Access to documents held by public bodies and the Protection of personal information**, it defines personal information as:

> For the purposes of this Act, personal information is sensitive if, due to its nature, in particular its medical, biometric or otherwise intimate nature, or the context of its use or release, it entails a high level of reasonable expectation of privacy.

Suggestion: Consider developing a clear definition for 'sensitive personal information' to assist in identifying and categorizing information that requires a greater level of care than other types of personal information. The definition could include reference to information relating to specific groups, such as minors, seniors, or vulnerable individuals, as well as categories of information that generally warrant a higher level of reasonable expectation of privacy, such as biometric data, information of an intimate nature, or medical information. Ultimately, it is the nature of the information that will determine if it should be deemed sensitive.

4.2 Sharing of personal information for connected or integrated service delivery

Issue:
Services offered by public bodies are increasingly integrated across departments and agencies. Members of the public often experience government as a single organization, rather than as separate departments or public bodies, and expect to be able to access programs and services quickly and efficiently.

MyGovNL is an example of a connected service model that provides individuals with a more centralized way to interact with government services. A clear legislative framework that supports connected or integrated services would help enable this type of citizen-centred service delivery while maintaining appropriate privacy safeguards.

A connected service model can also support a "tell us once" approach for certain categories of personal information. For example, where an individual provides or updates basic identity or contact information through a trusted government service, that information could become a single authoritative source for use by participating public bodies for approved service-delivery purposes. This would reduce duplication for individuals, improve accuracy and consistency across government systems, and reduce the need for individuals to repeatedly provide the same information to multiple public bodies.

There can be practical challenges and uncertainty for departments and public bodies when sharing personal information to support integrated services. Public bodies may be unsure whether the **Act** permits collection, use or disclosure in a particular service-delivery context, particularly where multiple public bodies are involved or where one public body is providing a service on behalf of another. This uncertainty can slow down service delivery and lead to inconsistent approaches. A specific provision in the **Act** could provide clearer authority for the collection, use and disclosure of personal information for defined connected or integrated services.

It is important that any such provision carefully consider and integrate a strong privacy by design approach to ensure that there are clear parameters for what can be shared, to whom, in what contexts, how such information is to be shared and secured and setting out any categories of personal information that may not be shared in a connected/integrated services model.

British Columbia recently introduced amendments to its **Freedom of Information and Protection of Privacy Act** which enables a streamlined sharing of personal information through a connected service provider. A connected service provider may collect, use and disclose personal information between other public bodies, to deliver specified services, such as establishing and maintaining an online platform to facilitate access to, and delivery of, services and programs of one or more public bodies; facilitating the sharing of personal information between public bodies; and identifying services and programs for which a person may be eligible.

British Columbia provides a useful model for consideration. Section 69.2 enables the designation of a provincial identity information services provider and authorizes services such

as identifying individuals, verifying identity, updating personal identity information, issuing physical or electronic credentials, and managing identity information services that public bodies may use to confirm identity. Section 69.3 similarly contemplates a connected services provider and a connected services platform to support the delivery of services across public bodies. British Columbia's Act also includes related collection authorities where personal identity information is collected to enable identity services or connected services.

Nova Scotia's new **Freedom of Information and Protection of Privacy Act** also provides a helpful example. Section 137 contemplates an identity information service provider model that can support government identity services, including the collection, use and disclosure of identity information for prescribed identity-management purposes. This type of provision could help clarify when a designated public body may verify an individual's identity, maintain or update core identity information, issue or support credentials, and make identity information available to other public bodies for approved service-delivery purposes. Any comparable authority in Newfoundland and Labrador's **Act** should be limited to clearly defined identity information, designated providers and participating public bodies, with safeguards to ensure the information is used only where necessary for identity verification, authentication, eligibility assessment or connected service delivery.

The concept of an identity information service provider is best understood as an enabling component of connected service delivery. British Columbia's section 69.2 highlights this approach by allowing a designated provincial identity information services provider to support identity services, including confirming identity, updating identity information and issuing credentials. Nova Scotia's section 137 similarly recognizes the role of a designated identity services provider in verifying identity, updating identity information and supporting physical or digital credentials. Including this concept within a broader connected service provision would help ensure that identity services are clearly tied to approved service delivery, rather than creating a separate or open-ended authority to share identity information.

Suggestion: Consider creating a clear legislative framework to enable connected or integrated service delivery, including authority to designate an identity information service provider as part of that framework. The identity information service provider should support, but not operate separately from, the broader connected service model by enabling identity proofing, identity verification, authentication, credential issuance, and the maintenance or updating of core identity information needed to deliver approved services across participating public bodies. This could include:

- authority to designate an identity information service provider within the connected or integrated service delivery framework;
- authority to designate a connected services provider or platform to coordinate approved services across participating public bodies;
- authority for participating public bodies to collect, use and disclose specified personal information where necessary to provide an approved connected or integrated service;
- a requirement that the categories of personal information and participating public bodies be clearly defined;
- authority to establish a single authoritative source for certain identity or contact information;

- clear authority for identity proofing, identity verification, authentication, credential issuance and the maintenance or updating of core identity information by a designated identity information services provider;
- safeguards requiring necessity, accuracy, security, transparency, information sharing agreements, privacy impact assessments, role-based access, audit logging and retention limits; and
- regulation-making authority to prescribe connected services, identity information, participating public bodies and any additional safeguards.

4.3 Data residency

Issue:
Data residency and data sovereignty are emerging privacy issues that have received increasing attention.

Data residency is the geographical location where data is stored, while **data sovereignty** is the legal authority and jurisdiction that governs that data. Foreign jurisdictions may lack robust privacy legislation, putting personal information at risk if it is stored in a foreign country or controlled by a foreign corporation. Foreign corporations may also be subject to demands by their government for personal information they hold.

As this is an emerging issue, it would be prudent to enact legislation that recognizes this risk and allows government to quickly respond through regulation.

The Government of Canada recently released its digital sovereignty framework. This framework seeks to achieve digital sovereignty not through strict data localization or domestic sourcing alone, but by ensuring the Government of Canada retains **control, security, resilience, and continuity of operations** through a combination of legal, contractual, supply chain, and technical measures.

While data sovereignty remains a complex issue that is continuing to evolve, data residency and cross-border transfers of personal information can be found in some public sector legislation within Canada.

Nova Scotia's new **Freedom of Information and Protection of Privacy Act** (coming into force in 2027) incorporates data residency requirements. Specifically, section 76 states:

> 76. A public body may not
>
> (a) disclose personal information outside of Canada;
>
> (b) store personal information outside of Canada; or
>
> (c) permit personal information in its custody or under its control to be accessed from outside of Canada,
>
> unless the disclosure, storage or access is in accordance with the regulations.

Nova Scotia's regulations are currently being drafted. By enacting a similar provision, this would allow government to draft regulations and respond effectively to data residency and data sovereignty issues.

Quebec's **Act respecting Access to documents held by public bodies and the Protection of personal information** requires public bodies to conduct a privacy impact assessment before releasing personal information outside Quebec. Section 70.1 states:

> **70.1.** Before releasing personal information outside Québec, a public body must conduct a privacy impact assessment. The body must, in particular, take into account
>
> (1) the sensitivity of the information;
>
> (2) the purposes for which it is to be used;
>
> (3) the protection measures, including those that are contractual, that would apply to it; and
>
> (4) the legal framework applicable in the State in which the information would be released, including the personal information protection principles applicable in that State.
>
> […]

Suggestion: Enact provisions requiring personal information to be stored within Canada, unless the disclosure, storage and access of personal information outside of Canada is authorized under regulations.

Consider including authority under s.116 that would authorize the Lieutenant-Governor in Council to establish regulations that address access and ownership of personal information outside of Canada.

Consistent with commentary at 3.2- Making the Act flexible as technology evolves of this submission, this will ensure that the legislation is responsive to the evolving technological landscape impacting privacy.

4.4 Clarity on minimizing collection

Issue:
Currently, information may be collected under the **Act** in three circumstances:

> (a) the collection of that information is expressly authorized by or under an Act;
>
> (b) that information is collected for the purposes of law enforcement; or
>
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

The provision on collection does not specify that public bodies must only collect the minimum amount necessary. This term appears around the use (66(2)) and disclosure (68(2)) of personal information but not the collection of personal information.

Provisions in New Brunswick, Manitoba and Yukon contain collection provisions which make the principle of minimum collection clearer.

Manitoba's collection provision contains a collection provision very similar to Newfoundland & Labrador, with 3 sources of authority that are very close to the **Act**. However, it also adds the following:

> **36(2)** A public body shall collect only as much personal information about an individual as is reasonably necessary to accomplish the purpose for which it is collected.

Suggestion: Consider clarifying s.61 of the **Act** to ensure that public bodies only collect the minimum amount necessary, similar to Manitoba's s.36(2).

4.5 Defining program or service for the purpose of PIA requirements

Issue:
Currently, the **Act** requires a PIA or Preliminary PIA to be completed on any new program or service:

> **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

The terms "program" and "service" are not defined under the **Act**. The ATIPP Office is occasionally required to make judgement calls on whether a particular activity qualified as a program or service. Some situations include:

- Changing the means of communication (e.g. a PDF vs a Gravity form)
- New sharing of personal information
- Issuing of an RFP
- One time sharing
- Minor administrative changes to an activity

There is limited interpretation or litigation around these terms.

In British Columbia (Finance) (Re), 2019 BCIPC 41 (CanLII), the following definitions of "program" were discussed:

- A course of activities or actions undertaken to achieve a certain result
- A set of related measures or activities with a particular long-term aim
- an operational or administrative program that involves the delivery of services under a specific statutory or other authority

"Service" is not a commonly used term in most Canadian access and privacy legislations as most use the terms "program or activity". There is some litigation in other contexts which defines service:

- "service" must mean something which is of benefit that is provided by one person to another or to the public 2023 HRTO 1166 (CanLII) | S.Y.L. v. Replay Marketing | CanLII

Suggestion: Define "program or service" under the act to clarify when a privacy impact assessment is required. Potential definitions could include:

- "Program means a course of activities or actions undertaken to achieve a certain result"

- "Service means any benefit provided by a government department to the public or to a group of people"

4.6 Privacy assessment requirement and triggers

Issue:
Across Canada, there is considerable variation in how jurisdictions approach privacy assessments. Some provinces and territories, including British Columbia, Alberta, Ontario, Quebec, Yukon, Nunavut, and Newfoundland and Labrador, have legislative requirements to conduct privacy assessments. However, the scope of those requirements differs. Some jurisdictions focus primarily on technology projects, information systems, or specific uses of personal information, while others apply a broader requirement to programs, services, or activities that involve personal information. Nova Scotia's **Freedom of Information and Protection of Privacy Act** (not yet in force) will make privacy assessments mandatory beginning in 2027. Section 53(1) of the revised legislation states:

> 53 (1) A public body shall (a) before undertaking or instituting a project, program, system or other activity involving the collection, use or disclosure of personal information, conduct a privacy assessment of the project, program, system or activity; and
>
> (b) before substantially changing a project, program, system or other activity involving the collection, use or disclosure of personal information, conduct a privacy assessment of the project, program, system or activity that reflects the anticipated change

The wording of this new provision makes it clear that assessments must be conducted prior to changes taking place. This is important because it can be difficult to provide meaningful privacy input on a project if it is already developed and decisions have already been made. Additionally, it includes a requirement to conduct privacy assessments on substantial changes that have a privacy impact. A major change to a project can result in significant privacy risks which should be reviewed and mitigated before implementation.

Suggestion: Amend the provision to clearly require:

- That privacy impact assessments (or, if appropriate, preliminary assessments) be completed and submitted before a new or significantly modified program, service, activity, or initiative is implemented.
- A privacy assessment be completed or updated when there are services that include significant updates or changes to existing programs and services that impact privacy.

4.7 Privacy of public body employees

Issue:
One of the principles of access and privacy laws is that the public has a right to know how government makes decisions and how it spends money. As such, employees of public bodies have certain elements of their personal information that has been determined to generally not be an unreasonable invasion of their privacy, such as information about their position and

remuneration as well as opinions or views given by them in their role as a public body employee, as set out in s.40(2)(f), (h) and (j).

While it is recognized that overall, disclosure of certain elements of public body employees' personal information is not an unreasonable invasion of their privacy, it is important to recognize that there may be extraordinary circumstances where such information could potentially be harmful, which in normal circumstances would not be an unreasonable invasion of most individuals' privacy. Such consideration is in fact embedded in the **Public Sector Compensation Transparency Act**.

This legislation requires an annual listing of all employees in departments and a number of agencies, boards, commissions, health care bodies, educational bodies and Crown corporations who receive total compensation of more than $100,000 in a year.

The **Act** provides a clear exemption process and factors for consideration. Specifically, it sets out that an individual employee, or category of employee, may be exempted from disclosure if disclosure could "reasonably be expected to threaten the safety, or mental or physical health of that employee;" this wording aligns with the section 37 exception. As part of the process undertaken annually, government issues a notice to all employees that this listing is being prepared and provides a timeframe for any individuals seeking an exemption to submit their request for exemption. This process allows for a more fulsome consideration of individual circumstances which may result in specific individuals being exempted from the disclosure listing. Each year there are a small number of employees who qualify for an exemption.

While the **Act** allows for notification to an individual (including a public body employee) where their personal information may be disclosed, this is often not used where the information being requested is set out in s.40(2) as not being an unreasonable invasion of their privacy. This situation, however, fails to account for specific circumstances that may be relevant in extraordinary circumstances. Often, the employee whose personal information has been requested is not aware of the initial request or the subsequent disclosure where that information is determined not to be an unreasonable invasion. This could mean that information that may be harmful to an individual based on unique and extraordinary circumstances could be disclosed without the individual's knowledge. In addition, it is very unlikely that the ATI Coordinator or executive would be aware of risks based on highly personal circumstances.

Were there a requirement, similar to the exemption process in the **Public Sector Compensation Transparency Act**, that meant that employees were notified where their personal information was being requested, even where it is believed not to be an unreasonable invasion of their privacy, those employees are then able to put forward any relevant information or evidence where they believe that disclosure would be harmful to their safety or mental or physical health.

Suggestion: Government is committed to protecting its employees and ensuring they are aware of requests that may impact them personally to ensure that the two principles of the Act are maintained – providing access to information while also protecting peoples' privacy (in this case the privacy of employees). Therefore, it is suggesting that the Committee consider establishing a clear employee notification process before information about an employee is

disclosed, including where disclosure of personal information would not normally be considered an unreasonable invasion of privacy, and giving employees a reasonable opportunity to identify safety or health risks before a public body makes a decision about disclosure.

Part 5 – Privacy Breach Management

Terms of Reference, Mandate Area 5: review the effectiveness of current privacy breach notification requirements and timelines; assess the adequacy of public body obligations for breach prevention, response, and reporting.

5.1 Definition of privacy breach

Issue:
ATIPPA, 2015 does not include an express definition of privacy breach. Section 64 addresses the protection of personal information and references breaches and notification requirements associated with breaches. It generally frames breach as "involving the unauthorized collection, use or disclosure of personal information" (s.64(4)). This does not capture instances where personal information may be accessed or disposed of without authorization.

Suggestion: Consider adding an express definition of privacy breach similar to s.78 of Nova Scotia's new **Freedom of Information and Protection of Privacy Act**, coming into force in 2027 which states:

> 78 (1) In this Section,
> […]
> "privacy breach" means, in relation to personal information,
> (a) theft or loss; or
> (b) collection, use, disclosure, access or disposal, whether intentional or unintentional, that is not authorized by this Act;

5.2 Privacy breach notification

Issue:
ATIPPA, 2015 currently requires public bodies to inform the Commissioner of privacy breaches. However, this requirement does not set out any general or specific requirements with respect to timing:

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

The provinces vary in terms of reporting requirements; however where there are reporting requirements there is generally a requirement to report within a reasonable or urgent time frame. For example, Alberta requires as follows:

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

Quebec's **Act respecting Access to documents held by public bodies and the Protection of personal information** includes somewhat similar language:

> 68.3 […] If the incident presents a risk of serious injury, the public body must promptly notify the Commission. […] [emphasis added]

The Federal Privacy Commissioner in 2020 provided commentary related to Quebec's Bill 64, an **Act to modernize legislative provisions as regards the protection of personal information**. This Bill included similar language to the above, requiring "prompt" notification to the Commission. The Federal Privacy Commissioner, in his written statement, recommended adjusting this language as follows:

> "However, we believe that the new legislation should stipulate that the CAI should be notified, "as soon as possible after an incident occurs". The reason is simple: speed is crucial for setting up, on an individual level, the appropriate protection measures following a breach of confidentiality."

While the provinces do not set out a specific time frame, it is also notable that GDPR requires notification to the commissioner within a specific time frame of 72 hours.

Privacy breaches take time to investigate and not all details may be immediately available. However, it would be useful to require public bodies to report breaches within a reasonable timeframe. Having an initial or early notification to the commissioner, even while the details of the breach are still being determined, is important. Early notification to the Commissioner is important because privacy breaches often require decisions before all facts are fully confirmed. Sharing available information early supports timely oversight, allows the Commissioner to provide guidance as the public body continues to investigate, and helps ensure that risks to affected individuals are identified and addressed as quickly as possible. Early notification also promotes transparency, accountability, and public confidence in the public body's response.

For those breaches with a higher level of risk, a specified time frame may be appropriate.

Suggestion:

- Consider requiring notification to the commissioner of all privacy breaches as soon as possible after an incident occurs once they are discovered.
- Consider requiring notification to the commissioner of breaches involving a risk of significant harm within a specific time frame after being discovered.

Part 6 – Public Body Practices and Accountability

Terms of Reference, Mandate Area 6: evaluate the privacy management frameworks of public bodies, including the role of Privacy Impact Assessments and mandatory training; consider whether additional oversight or enforcement mechanisms are needed.

6.1 Designate privacy officer

Issue:
Section 110 of the **Act** specifically sets out the requirement to designate someone as a coordinator to:

> (a) receive and process requests made under this Act;
> (b) co-ordinate responses to requests for approval by the head of the public body;
> (c) communicate, on behalf of the public body, with applicants and third parties to requests throughout the process including the final response;
> (d) educate staff of the public body about the applicable provisions of this Act;
> (e) track requests made under this Act and the outcome of the request;
> (f) prepare statistical reports on requests for the head of the public body; and
> (g) carry out other duties as may be assigned.

Traditionally, in government the coordinator was also responsible for privacy-related matters as well, including responding to privacy breaches, providing training on privacy obligations and preparing privacy assessments of programs and services. This function is no longer part of the role of the ATI coordinator within government given the demands associated with receiving and responding to access requests.

The role should support privacy accountability across the public body, including advice on privacy assessments, breach response, information-sharing initiatives, emerging technologies, privacy training, and the development of privacy policies and procedures.

Currently, two Canadian jurisdictions require the designation of a privacy officer or someone responsible for the protection of personal information. S.84(1) of Yukon's **Access to Information and Protection of Privacy Act** requires that the minister appoint an access and privacy officer. Quebec's **Act respecting Access to documents held by public bodies and the Protection of personal information**, s.8 requires the head to designate someone to be responsible for the protection of personal information.

Quebec's Act also includes a requirement to have a committee on access to information and privacy protection:

> 8.1. Within a public body, a committee on access to information and the protection of personal information is responsible for supporting the body in the exercise of its responsibilities and the performance of its obligations under this Act. The committee shall also exercise the functions entrusted to it by this Act.
>
> The committee is under the responsibility of the person exercising the highest authority within the public body or, in the case of a government department, of the deputy minister and, in the case of a municipality, a professional order or a school service

> centre, of the director general. It is composed of the person in charge of access to documents, the person in charge of the protection of personal information and any other person whose expertise is required, including, if applicable, the person responsible for information security and the person responsible for document management.
>
> A government regulation may exempt a public body from the obligation to establish such a committee or modify a body's obligations according to criteria it defines.

Other jurisdictions require the creation of privacy management programs, the details of which are set out in either Minister's direction or prescribed guidelines (British Columbia's **Freedom of Information and Protection of Privacy Act**, s.36.2; Alberta's **Protection of Privacy Act**, 2.25(2)). Those directions/guidelines require the designation of a privacy officer.

Suggestion: Consider including a requirement for public bodies to designate a privacy officer or privacy lead responsible for supporting compliance with the privacy provisions of the **Act**, with flexibility for smaller public bodies to meet this requirement.

Part 7 – Public and Public Body Experience

7.1 Cross-reference summary

Terms of Reference, Mandate Area 7: gather feedback on the experience of individuals and public bodies operating under the **Act**.

Public and public-body experience is addressed throughout the submission. Applicant experience is discussed in sections 1.2, 1.3, 1.8, 1.19, 1.22, 2.4, and 2.5. Public body operational experience is discussed in sections 1.1, 1.4 to 1.7, 1.9, 1.17, 1.20, 2.1 to 2.7, 4.5 to 4.7, 5.2, and 6.1. Municipal experience is summarized in Part 9.

7.2 Government access and privacy professionals' feedback

In preparing this submission, government consulted directly with access and privacy professionals within the ATIPP Office, as they have direct experience with the application and administration of the Act. Through these consultations, key themes consistent with the 2020 Review Committee findings emerged relating to access and privacy:

Access provisions of the **Act**:

1. Timelines - individuals felt the timeline no longer reflects the volume, complexity, and sensitivity of modern access requests (e.g. requiring clarification from applicants, timelines for submitting applications for approval to disregard requests from the OIPC, the use of artificial intelligence in framing requests, etc.).
2. Administrative burden – this included internal redundancies, issues with various tools/technology used to process requests, as well as legislative requirements such as the advisory response required under s.15 of the **Act**.
3. Costs – participants questioned whether current fee provisions adequately reflect the resources required to process access requests. Many noted that locating electronic records is generally less resource-intensive than reviewing and redacting records, but current cost provisions do not recognize this shift.
4. Proactive disclosure - this emerged as one of the strongest opportunities to improve efficiency while maintaining openness and transparency. There was strong support for routinely publishing commonly requested records and creating a centralized approach to proactive disclosure across government.
5. Legislative clarity - individuals identified several areas where additional clarity or legislative amendments may be beneficial, including workplace investigations, third-party consultations, employee privacy, custody and control issues, approval authorities, and production of records during OIPC investigations. Individuals identified workplace investigations (s.33) as one of the most challenging areas within the **Act**.
6. OIPC processes, complaints and oversight - individuals recognized the important oversight role of the OIPC but identified opportunities to improve complaint, audit, and review processes. They suggested greater consistency, communication, and

transparency would help public bodies better understand expectations and improve future practices.

Privacy provisions of the **Act**:

1. Modernization – individuals viewed modernization as necessary to address emerging issues such as digital government, cloud tools, AI and cybersecurity.
2. Clearer legislative authority and rules – individuals identified concerns that the current framework relies too heavily on policy, case law and interpretation.
3. Privacy assessment timing – individuals identified a need for privacy assessments to occur at an early stage of planning in order to influence programs, with mandatory assessment triggers and post implementation reviews where appropriate.
4. Breach reporting – individuals identified a need for clarity on breach recognition and reporting, as well as better employee awareness.
5. Contract priorities – individuals identified a need for consistency in contracts, monitoring older contracts and specific guidance on AI, cloud use, and data residency.
6. Children and minors – individuals identified the need to address children's privacy specifically, including issues such as clarity and consent.

Part 8 – Schedule A Review

Terms of Reference, Mandate Area 8: review the list of provisions in **Schedule A** to determine the necessity of their continued inclusion.

8.1 Sections of legislation listed in Schedule A

Schedule A includes provisions from other legislation that prevail over ATIPPA, 2015 in the event of a conflict. It is government's position that the majority of these provisions should remain in Schedule A – they serve to ensure processes unique to those pieces of legislation remain and that requirements under ATIPPA, 2015 do not have unintentional negative impacts on the important functions these provisions serve. We would note that there are 4 distinct provisions currently included in Schedule A that government has indicated it is supportive of removing from Schedule A:

- S.8(1) of the **Evidence Act**
- S.5(1) of the **Fish Inspection Act** (in conjunction with recommendation 47)
- S.4 of the **Fisheries Act** (in conjunction with recommendation 47)
- S.18 of the **Workplace Health, Safety and Compensation Act**

Government would highlight the reference in the Wells Report in terms of the approach in assessing the sections included under Schedule A. Specifically, the Committee stated:

> "The Committee agrees that it would be good practice to review the list in conjunction with each five-year review. We do not agree that it is desirable to expressly state that an onus is on each public body concerned to make a convincing case for continued inclusion of provisions for which that public body had responsibility. That would be tantamount to automatic exclusion unless somebody from each public body concerned appeared and made a convincing case every five years, whether or not it was obvious that the provision should remain. A better approach would be for a committee doing a five-year review to indicate which provisions, if any, it believed should be considered for removal from the list. In that way the public body concerned would be fore warned and take steps to make a convincing case for continued inclusion at the next five-year review. […]"

In his 2020 report, Justice Orsborn further considered this approach, stating:

> "As I have indicated on a number of issues, I consider the report of the Wells Committee to be the foundation of the current Act. Unless persuaded by five years of experience, the need for clarification, by changing circumstances, or other compelling reason, I do not propose to make recommendations to disturb this solid foundation."

It is government's position that, except for those 4 sections outlined above, all other sections currently listed in Schedule A should be maintained.

8.2 The role of Schedule A around privacy

Issue:
Section 7(2) of **ATIPPA, 2015** states:

> Notwithstanding subsection (1), where **access to a record** is prohibited or restricted by, or the right to **access a record** is provided in a provision designated in Schedule A, that provision shall prevail over this Act or a regulation made under it. [emphasis added]

Schedule A sets out a number of different provisions that prevail over **ATIPPA, 2015**. While many of these provisions are about the access side of the act, some provisions refer to privacy issues as well.

For example, Schedule A lists sections 64 to 68 of the **Adoption Act, 2013** as one of the Acts that prevails over the **Act**:

> (a) sections 64 to 68 of the **Adoption Act, 2013**;

Section 64 of the **Adoption Act, 2013** states

> **64.** Notwithstanding the **Access to Information and Protection of Privacy Act, 2015** and the **Privacy Act** (Canada), the **collection of, use of, disclosure of and access to information in records** created by or received by the department in the exercise of all powers, duties and functions under this Act, regardless of where the information or records are located, shall be governed by this Act. [emphasis added]

The **Adoption Act, 2013** exemption includes provisions both dealing with exemption from access to information provisions and privacy provisions. However, on the privacy side the **Adoption Act, 2013** does not address some important privacy matters such as breach reporting and reasonable safeguards.

While adoption records are the example given, the same concerns may apply to other exemptions set out in Schedule A.

Suggestion: Consider modifying section 7 of the **Act** to clarify whether a provision being listed Schedule A creates an exemption for the access provisions of the act, or both the access and privacy provisions of the Act.

Part 9 – Municipalities

The 2020 submission included a dedicated section on municipal capacity issues, cutting across several mandate areas above (timelines, vexatious requests, costs, local public body confidences, and designation of head/coordinator).

9.1 Municipal issues cross-reference

Municipal capacity and implementation issues are addressed in section 1.17, section 1.19, section 1.20(ii), section 2.1, section 4.7, and section 6.1. The proposed approach emphasizes proportionate requirements, delayed implementation where needed, centralized or shared support models, and monitoring of actual demand before additional resources are established.

Municipalities vary significantly in size, staffing, administrative capacity, information management practices and access to legal, privacy and technology expertise. Many municipalities in this province are serving aging communities and operate with limited staff (i.e., often single-person or part-time administrative teams) and significantly shrinking volunteer capacity. Any new or expanded obligations will need to therefore recognize these real and evolving operational differences across communities, while supporting consistent access and privacy protections across the province. A one-size-fits-all approach places disproportionate pressure on smaller municipalities, particularly when requirements involve items like privacy assessments, or breach reporting, etc. Municipalities continue to note to government the significant staff hours required to identify, local, review, sever, and manage records, which they note is often diverting limited municipal resources away from core daily operations,

Implementation of any new or expanded obligations should be guided where possible by proportionality, with obligations scaled to the municipality's operations, the sensitivity and volume of personal information held, the level of risk associated with its programs and services, and the municipality's ability to meet new requirements without unreasonable disruption to essential operations. While access rights must remain meaningful, ATIPPA implementation should continue to help ensure that municipalities have appropriate tools and guidance to manage access and privacy obligations in a way that protects local governments and their staff from abusive or malicious conduct and supports a safe and respectful municipal workplace.

Digital capacity also needs to be considered. Many municipalities do not maintain websites, so related proactive disclosure requirements should include flexible options. The impact of new municipal obligations for access and privacy should be considered before determining whether further cost reimbursement programs or centralized supports are required.

Conclusion

In conclusion, this submission reflects the importance of maintaining an access to information and privacy framework that is clear, practical, accountable and responsive to the needs of applicants, public bodies and the public. The recommendations and suggestions outlined throughout this submission are intended to support timely and meaningful access to information, strengthen privacy protection, improve consistency in public body practices and ensure that the **Act** continues to operate effectively in practice.


Newfoundland
&
Labrador