



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Access to Information and Protection of Privacy Act, 2015 Review

**Submission of the
Information and Privacy Commissioner for
Newfoundland and Labrador**

October 9, 2026

Intentionally Left Blank

Table of Contents

INTRODUCTION	1
REVIEW OF 2020 RECOMMENDATIONS.....	5
ACCESS TO INFORMATION PROVISIONS – EXCEPTIONS TO ACCESS.....	5
Solicitor-Client Privilege	5
Settlement Privilege.....	14
Workplace Investigations	15
Third Party Business Interests	25
Public Interest Override	36
Information Technology Security.....	37
ACCESS TO INFORMATION PROVISIONS - TIMELINES	40
Access Request Timelines and Extensions	40
Overdemand by Applicants and Disregard	45
ACCESS TO INFORMATION PROVISIONS – ADMINISTRATIVE PROCEDURES	48
Informal Resolution Procedure	48
Access to Information Complaints and Appeals	50
Commissioner Vacancy	50
PRIVACY SAFEGUARDS AND EMERGING TECHNOLOGIES.....	53
Artificial Intelligence.....	53
Biometric Data	56
Surveillance Technologies.....	63
PERSONAL INFORMATION PROTECTION.....	65
Privacy and Political Parties	65
Enhanced Safeguards for Sensitive Categories of Data	69
Rights of a Minor	70
Indigenous Issues	70

PRIVACY BREACH MANAGEMENT	71
Privacy Breach Notification Requirements and Timelines	71
Public Body Breach Prevention, Response, and Reporting	77
PUBLIC BODY PRACTICES AND ACCOUNTABILITY.....	82
Privacy Management Frameworks	82
Privacy Impact Assessments.....	84
Mandatory Training.....	90
Additional Oversight or Enforcement Mechanisms	94
PUBLIC BODY PRACTICES AND ACCOUNTABILITY – OTHER SIGNIFICANT ISSUES	96
Duty to Document	96
Publication Schemes, Information Directories and Proactive Disclosure.....	99
ATIPPA, 2015 "SCHEDULE A" REVIEW	101
Appendix A – OIPC’S Consideration of the 2020 Statutory Review Recommendations.....	105
Appendix B – OIPC’s 2020 Submission on Solicitor-Client Privilege.....	118
Appendix C –OIPC’s 2020 Submission on Access to Information Complaints and Appeals	126
Appendix D – OIPC’s 2020 Submission on Artificial Intelligence.....	131
Appendix E – OIPC’s 2020 Submission on Indigenous Issues.....	135
Appendix F – List of Recommendations	136

INTRODUCTION

Newfoundland and Labrador is fortunate to have one of the best access to information laws in Canada. This province consistently ranks first in the Centre for Law and Democracy's annual Right to Information Laws [rating](#). Where other provinces have reduced access to information, have created broad exceptions that apply to swaths of records, or have made it unduly burdensome in time or money for an individual to bother applying for records at all, this province has taken access rights seriously. The decision to protect and promote access to information means there is less disinformation and misinformation in the public discourse. This in turn leads to a more informed and engaged public who are better able to participate in open debate, and in democracy.

The **Access to Information and Protection of Privacy Act, 2015** was a landmark piece of legislation. It underwent a comprehensive statutory review by former Honourable Chief Justice David Orsborn, Committee Chair in 2020. As a result of the fact that there were no amendments following that review, we now have additional data and experience: a total of eleven years of ATIPPA, 2015 as a well-functioning statute. Based on that experience, our highest priority is to see the current provisions of ATIPPA, 2015 continue as they are. While there are sections of the Act where clarity could be provided, it is essential to ensure that access and privacy rights, and the oversight provided by this Office, are not diminished. As an Office dedicated to the oversight of this statute, we believe that there are only a select few necessary changes to ATIPPA, 2015, none of which would impact the model or processes of how the Act functions. Our priority recommendations focus on areas where ATIPPA, 2015 requires greater clarity or is an emerging issue that warrants new legislative provisions to provide necessary guidance. In particular, we would like this Review Committee to focus on recommendations for solicitor-client privilege, workplace investigations, overdemand, disregards, artificial intelligence, and political parties.

Our submission has focused on the terms of reference that were provided to the Review Committee and other key issues that we believe warrant additional attention as part of this review. Firstly, this Office has struggled with our ability to provide effective oversight of section 30 (legal advice) as an exception to access to information. The courts have now made it

abundantly clear that unless ATIPPA, 2015 provides express authority for the commissioner to review records where there has been a claim of solicitor-client privilege, that those records will not be reviewed without resort to the courts. The most recent jurisprudence has further established that even the courts will not review the records unless there is evidence that the privilege was wrongly claimed, yet no party other than the public body will typically possess that evidence. This has given public bodies, of all levels of sophistication, the ability to simply claim section 30, with barely more than a statement that section 30 applies, and there is no effective recourse for an applicant to challenge that assertion. It has become more apparent over time that certain public bodies have used section 30 to deny disclosure simply to undermine our ability to fulfil one of the purposes of the Act, which at section 3(2)(a) is independent review of decisions made by public bodies under the Act. Transparency and accountability are also purposes of ATIPPA, 2015 referenced in section 3. There is no way to square any interpretation of the term accountability with a circumstance where public bodies can make decisions to deny access to information with no oversight. While we absolutely appreciate the sanctity of solicitor-client privilege, we formally call on the government to enact provisions that a reasonable member of the public would agree is an appropriate method for public bodies to discharge their burden of proof when they refuse access to information claiming solicitor-client privilege. Saying “trust me” is not accountability, and members of the public who use the Act can plainly see that.

Another area we would like to highlight is section 33 (workplace investigations) as that section has created issues whereby clarity would be beneficial for all parties involved. These investigations often involve sensitive personal information, and public bodies need a better framework to make decisions around disclosure.

We note that since the voters list privacy breach that occurred in Alberta, much attention has finally turned to the issue of political parties and the rules around their collection and use of voters’ personal data. The Alberta breach was significant and is now subject to multiple investigations. Privacy regulation needs to apply to political parties, and it is our hope that the recommendations from this submission will be taken up to ensure voter personal information is protected in this province.

The terms of reference for this review focus partly on privacy considerations, and we were asked to ponder whether additional statutory provisions are warranted. This is a difficult question to answer in a vacuum, without having some hint as to government's intended policy direction. The challenge is that the ever-increasing availability of newer and more advanced technology continually invites public bodies to consider the ways in which those technologies can be used in service delivery. In many cases, this involves novel collections, uses, and disclosures of personal information in ways which can increase privacy risks. Sometimes public body officials, with the best of intentions, have not been able to, or perhaps do not have the capacity to, adequately assess these risks.

That is why, in this submission, we recommend several measures that will help ensure that there is some degree of oversight before such policies and programs are put into place. Such measures include expanded privacy impact assessment (PIA) requirements; the establishment of new algorithmic impact assessment (AIA) requirements; the creation of published registries for both PIAs and AIAs; and, giving the Commissioner the authority to obtain, review, and provide comments on both types of assessments. Another such measure would involve a return to the past practice of providing draft bills containing implications for access or privacy to the Commissioner for review and comment prior to the bill being tabled in the legislature. All of these measures could harness the expertise of the OIPC to assist public bodies with advice before the implementation of policies or programs that could seriously impact the privacy rights of Newfoundlanders and Labradorians.

The statutory timelines set out in the Act cause consternation for everyone involved in the access to information system. Complainants tell us that their access request took too long, that we granted too many extensions, or that public bodies do not assist them enough. Public bodies tell us that requests are more numerous and more complex than ever before and that timelines or deadlines are too short for their minimal resources. As the regulator we see both sides of this argument and work diligently to ensure fairness to all those involved. It is our hope that the recent expansion of the ATIPP Office will assist government departments who encounter the largest number of access requests. On balance, we believe that the extension and disregard processes already set out in the Act are very effective in both ensuring timely access and being mindful of public body challenges, and we ask that they remain unchanged.

The exception to this is we do support an increase to the number of business days that a public body has to apply to our Office for a disregard. We believe that the timeline here can be increased without interfering with an applicant's access rights.

We have strong professional connections with those who work in access and privacy across this country. We know that every jurisdiction in Canada has some struggles with access to information, regardless of their legislated timelines, whether there are fees involved, and regardless of the overall strengths and weaknesses of their laws. It simply goes with the territory. The job of access to information coordinator will always be a challenging one, and even in those jurisdictions where the statutory timelines are longest, where the costs are high, and when the exceptions are broad, coordinators will still be challenged to keep up with the workload. We are of the view that the benefits to be gained by public bodies from pulling back on the much-lauded provisions of ATIPPA, 2015 are meagre. When weighed against the loss of public trust and confidence in our government and public institutions that will likely result, it is clear to us that there is little to be gained, and much to be lost.

ATIPPA, 2015 is a source of national and international pride for Newfoundlanders and Labradorians. It is a "made in Newfoundland and Labrador" law that was not copied and pasted from elsewhere, and which continues to be implemented with a comparatively small budgetary investment. Those who work in all facets of this field have demonstrated over the past eleven years that this jurisdiction can be a leader in transparency and accountability, at a time in this world when democracy itself is under threat. Our plea is that we need to be able to say after this review is over, and after any resulting amendments, that Newfoundland and Labrador continues to hold the torch high, for transparency, for accountability, and for democracy.

REVIEW OF 2020 RECOMMENDATIONS

Terms of Reference Request: Consideration of the 2020 Statutory Review recommendations issued by the Honourable David B. Orsborn for applicability or revision.

Our Office conducted a comprehensive review of the 2020 Statutory Review recommendations ([Summary of Recommendations](#)) issued by the Honourable David B. Orsborn. To assist the Review Committee in readily identifying our Office's position on each recommendation, we developed a chart ([Appendix A](#)) that identifies each recommendation, and our Office's position.

For those recommendations on which our Office has taken a position, the chart indicates whether we agree or disagree and, in some cases, provides a brief rationale. Where our Office has identified a recommendation that warrants further discussion, the chart references the page in our submission where the matter is addressed in greater detail. Where “no comment” is indicated, this reflects our Office’s determination that the recommendation does not directly engage matters within our mandate or expertise, or that our Office has no specific concerns or comments regarding the recommendation.

Recommendation

Recommendation 2026-1: See [Appendix A](#) for OIPC’s position regarding the 2020 Statutory Review Recommendations.

ACCESS TO INFORMATION PROVISIONS – EXCEPTIONS TO ACCESS

Terms of Reference Request: Review **exceptions to access**, timelines for response, and the effectiveness of current administrative procedures and the current cost schedule.

Solicitor-Client Privilege

Background

Our prior submissions regarding solicitor-client privilege outline the historical background regarding our authority to review records and the evolution of that authority over time. As this

context remains relevant, our 2020 submissions on solicitor-client privilege are attached as [Appendix B](#).

Amendment Required to Restore Authority

The question of whether the Commissioner **should** have the authority to compel the production of records subject to a claim of solicitor-client privilege has been examined extensively during both the 2014 and 2020 statutory reviews. While the Review Committee may receive submissions arguing against providing the Commissioner with this authority, previous statutory reviews have consistently recognized the authority to review such records is necessary for the Commissioner to effectively carry out their oversight and investigative functions. Accordingly, both Review Committees recommended that the legislation expressly provide the Commissioner with the authority to compel the production of records over which solicitor-client privilege is claimed.

Since the release of the 2020 Statutory Review Report, the Newfoundland and Labrador Court of Appeal, in [Newfoundland and Labrador \(Information and Privacy Commissioner\) v. Newfoundland and Labrador \(Justice and Public Safety\), 2023 NLCA 27](#), determined the language currently used in ATIPPA, 2015's production provision, section 97(1)(d), is insufficient to abrogate solicitor-client privilege. Although the Commissioner's ability to compel the production of records subject to solicitor-client privilege has fluctuated over the years with various court decisions and statutory amendments, this decision makes it clear that ATIPPA, 2015 does not currently grant this authority. **Accordingly, for the Commissioner's authority to be restored, ATIPPA, 2015 must be amended to expressly and unequivocally authorize it.**

Before considering how the Act should be amended, it is necessary to examine the circumstances and surrounding context that give rise to the need for the amendment. The following sections review both our Office's historical experience with solicitor-client privilege claims and the accountability concerns that have emerged following recent judicial decisions. This context is important in evaluating how the Act should be amended.

Past Evidence of Overly Broad Claims

Following the decision of [Newfoundland and Labrador \(Information and Privacy Commissioner\) v. Newfoundland and Labrador \(Attorney General\), 2011 NLCA 69](#) which, at that time affirmed the Commissioner's ability to compel and review records, 14 files had been held in abeyance pending the outcome of this decision. Once the records were provided to the Commissioner and independently reviewed, it became clear that the claims of solicitor-client privilege were overly broad. In the majority of those files, more than half of the records claimed to be subject to solicitor-client privilege did not qualify for the exception. In most cases, public bodies accepted our Office's assessment, withdrew their claims, and voluntarily released the records.

The 2011 Court of Appeal decision addressed the Commissioner's authority to compel production of records. Once the Court confirmed that authority, the matter returned to OIPC for an independent review of the records at issue. Following that review, our Office issued [Report A-2013-004](#), which demonstrated that the Department's assurances regarding its claims of solicitor-client privilege were largely unsubstantiated. As noted in the Report, the majority of the records withheld on the basis of solicitor-client privilege did not, in fact, qualify for the exception:

It is clear that had the Department of Justice, in fact, reviewed this file on a "document-by document basis" at the outset, records would have been released to the Applicant prior to her initiation of a Request for Review with this Office. The Court of Appeal points out that by the very nature of the matter, it should have been clear to the Department that a more in-depth review of the records was required prior to claiming section 21¹. The initial review by my Office indicated that over 400 pages of records, on their face, did not meet the parameters to be protected by solicitor-client privilege. This amounted to more than half of the responsive records. The Department's attempt to claim solicitor-client privilege to withhold publicly available material such as legislation and government human resource manuals and policies did not come close to meeting the standard that I expect from the Department of Justice, especially given that it was the lead Department responsible for the ATIPPA at the time, and therefore responsible for setting the standard for all other public bodies.

¹ Section 21 was the solicitor-client privilege exception in the version of ATIPPA that existed prior to ATIPPA, 2015 coming into force.

The Department accepted the recommendations from that Report and provided additional records to the Applicant which had previously been withheld under a claim of solicitor-client privilege. The above experience clearly demonstrates that assurances from public bodies regarding claims of solicitor-client privilege were not always substantiated and that the extent of the over-claiming only became apparent once the records themselves were subject to independent review.

Alternative Forms of Evidence

As noted above, as a result of the Court of Appeal's recent decision, [Newfoundland and Labrador \(Information and Privacy Commissioner\) v. Newfoundland and Labrador \(Justice and Public Safety\), 2023 NLCA 27](#), the Commissioner is no longer able to compel production of, and examine, records withheld under section 30 for the purpose of determining whether solicitor-client privilege has been properly claimed. In carrying out its oversight mandate since that decision, our Office has been limited to relying on public bodies to either voluntarily provide records for review or to provide alternative evidence, such as sworn affidavits and detailed descriptions of the records, to substantiate the privilege claim.

Regarding affidavit evidence, the 2020 Statutory Review Report at page 121 anticipated this approach to alternative forms of evidence, stating:

I expect that if public bodies, in good faith, follow the suggestion of Harrington, J.A. and support any claim of solicitor-client privilege with a solicitor's affidavit and an appropriate listing and description of each document, any OIPC order for production would be rare.

The Report further states at page 123:

I would expect that any public body acting in good faith in asserting this position would, in the first instance, provide the commissioner with the solicitor's affidavit and listing referred to above. Should the OIPC not be satisfied as to the claim for privilege and the context of the advice, the matter should be considered as a decision by the public body to refuse access and proceed accordingly.

In practice, however, where our Office has sought sworn affidavit evidence or other detailed information to substantiate claims of solicitor-client privilege, public bodies, and government departments in particular, have often declined to provide such evidence. Instead, those public

bodies have taken the position that the assertion of a claim of solicitor-client privilege is sufficient to establish the application of the exception.

As a result, our ability to meaningfully assess the validity of privilege claims has been significantly constrained, despite historical experience demonstrating that assurances regarding solicitor-client privilege have not always proven reliable when subjected to independent scrutiny of the records themselves.

Recent Court Decisions and Alternative Forms of Evidence

In [Newfoundland and Labrador \(Justice and Public Safety\) v. Newfoundland and Labrador \(Information and Privacy Commissioner\), 2022 NLSC 59](#), it was clear that the then Commissioner advised the Department that, rather than producing the records themselves, it could provide an affidavit describing the records and setting out sufficient information to permit an assessment of whether solicitor-client privilege had been properly claimed. The Department declined both options. The resulting decision confirmed that the Commissioner lacks authority under ATIPPA, 2015 to compel production of records over which solicitor-client privilege is claimed, a conclusion that was subsequently upheld on appeal.

Of particular significance, however, is Justice MacDonald's commentary regarding the Commissioner's ability to seek alternative evidence in support of a privilege claim. He stated:

[61] I would also have concerns about the information the Commissioner would require in a letter or affidavit. What is “an appropriate ... description of each document”? This could be problematic if disclosure of the description in itself abrogates solicitor-client privilege.

While the issue was not directly before the Court, these comments call into question the Commissioner's longstanding ability to seek supplementary evidence, such as affidavits, to assess whether a claim of solicitor-client privilege has been properly asserted. Historically, where review of the records themselves was unavailable, obtaining alternative evidence provided at least some mechanism for independent scrutiny. Justice MacDonald's comments raise uncertainty as to whether even this limited form of review remains available.

The concern became more pronounced in [Newfoundland and Labrador \(Office of Women and Gender Equality\) v. Newfoundland and Labrador \(Information and Privacy Commissioner\), 2025 NLSC 70](#). In that matter, this Office argued that if the Commissioner could not review records subject to solicitor-client privilege, surely the Court itself should undertake that review. Justice O'Flaherty accepted that the Court possessed such authority but held that it could not be compelled to exercise it under ATIPPA, 2015. He further declined to review the records in issue, finding no basis to question the public body's assertion that solicitor-client privilege applied.

Notably, the public body did not provide the Commissioner with either the records themselves or affidavit evidence supporting its privilege claim. As described by the Court:

[4] The Commissioner requested that WGE disclose the solicitor-client privileged records for his review, or alternatively provide evidence by affidavit in support of its privilege claims. Relying on a decision of this Court, WGE refused both requests. WGE instead provided representations to the Commissioner that identified the records redacted, asserted that the redactions were subject to solicitor-client privilege, and advised the redactions were reviewed and confirmed by legal counsel.

The evidentiary record therefore consisted of written representations only. A sworn affidavit was neither before the Commissioner nor the Court to substantiate the claim of solicitor-client privilege. The representations made did not identify the lawyers who reviewed the records, nor did they describe the nature of their review, or provide particulars that would permit meaningful assessment of whether solicitor-client privilege properly attached to each record.

Despite the absence of sworn affidavit evidence about the solicitor-client privilege claim, the Court concluded:

[117] In the absence of any evidence or argument to suggest it was necessary to view the solicitor-client privileged documents to determine the validity of the privilege claim I would decline to do so.

This reasoning creates a significant practical difficulty. If neither the Commissioner nor the complainant can review the records, and if public bodies are not required to provide affidavit evidence to substantiate the claim, it is unclear how evidence capable of challenging the privilege claim could ever come to light. The effect is that the evidentiary burden appears to

shift to the complainant (or Commissioner) to demonstrate that a privilege claim may be invalid, while the information necessary to raise such a challenge remains solely within the control of the public body asserting the privilege.

It is important to recall that an appeal of an access to information decision by a public body is not a civil dispute between two equal parties. It occurs within a statutory context which establishes a public right of access with limited exceptions (sections 3 and 8), a statutory burden of proof (section 43), and independent oversight of decisions by public bodies as a stated purpose of the Act (section 3). The rights established in ATIPPA, 2015 exist partly because governments and citizens are not on an equal footing. Governments can make decisions that affect people, and transparency and accountability are fundamental means by which the public can be given agency and participate meaningfully in their democracy despite that imbalance. The current jurisprudence has placed us in a circumstance where the right of government and other public bodies to withhold information without meaningful oversight overrides the rights of individual citizens under ATIPPA, 2015, and in certain instances renders null the explicitly granted rights of access, burden of proof, and independent review of decisions.

Accountability Gap

A significant accountability gap currently exists for records over which solicitor-client privilege is claimed. Following the decisions in [Justice and Public Safety](#) and [Office of Women and Gender Equality](#), public bodies effectively determine for themselves whether the privilege applies. The Commissioner cannot review the records or compel evidence substantiating the claim, and the courts are accepting assertions as evidence and declining to independently examine the records. While solicitor-client privilege is a fundamental right that warrants strong protection, there is currently no effective mechanism for independently verifying whether the privilege applies.

As noted in [Report A-2026-030](#), recent court decisions have effectively reversed the statutory burden of proof when there is a claim of solicitor-client privilege. Rather than requiring a public body to establish that solicitor-client privilege applies, the burden of proof now rests with the complainant (or the Commissioner), to establish that solicitor-client privilege was wrongly

claimed. This Report states that such a burden "would rarely be possible to meet given that the evidence would likely be contained within the records themselves, which courts have decided that no one, but the public body may see." The practical consequence, as noted in the Report, is a significant reduction in the Commissioner's ability to independently scrutinize claims of solicitor-client privilege and provide meaningful oversight:

- [26] Most public bodies operate in a political context. Clearly there are times when public bodies are motivated to refuse access to information to avoid embarrassment, scandal, or simply accountability. Under the present circumstances, we now have a black hole into which records can go that will never see the light of day, and no independent party can adequately assess whether the public body was within its right or not to withhold them. With recent jurisprudence requiring this Office to accept mere assertions by the public body as sufficient to ground claims of solicitor-client privilege, the ability of the Commissioner to provide meaningful oversight and ensure compliance with the Act is significantly diminished.
- [27] Where the burden on the public body to prove a claim of solicitor client is so low, and there lies no mechanism for oversight, there is nothing to deter a public body from applying section 30 to any record of its choosing and simply asserting that it has been properly applied.

The current approach to solicitor-client privilege claims creates a significant accountability gap, leaving the Commissioner unable to meaningfully assess or verify whether records have been properly withheld. Rare circumstances will emerge from time to time in which either the content of the access request itself or the actions of the public body may establish enough evidence to allow the Commissioner to conclude that the privilege may have been wrongly claimed, despite not having access to the records. Such was the case in [Report A-2026-031](#). The only process available under the statute to the Commissioner in such cases is to recommend disclosure of all the records in doubt (even if it is possible that some may be legitimately privileged), to trigger a review by the courts. Based on recent jurisprudence, however, it is unclear whether a court will actually review the decision of the public body beyond accepting a mere assertion. Furthermore, the various deadlines in ATIPPA, 2015, including those that apply to the Commissioner's review, demonstrate that the entire construction of ATIPPA, 2015 is intended to facilitate timely access. The majority of complaints received by OIPC are resolved informally within weeks or are concluded at most within 65 business days via Commissioner's Report. Even if court were a means to guarantee independent review of decisions by public bodies when there is a refusal of access based on

solicitor-client privilege, the lengthy time frames involved mean that in many cases the information may no longer be relevant by the time the process concludes, thus depriving citizens of their right of access to information.

2020 Recommendations

The 2020 Review Committee sought to balance the protection of solicitor-client privilege with meaningful independent oversight by recommending that records be produced to the Commissioner only where production is "absolutely necessary" to assess a claim of privilege. That recommendation appears to have been based on the assumption that public bodies would substantiate privilege claims through solicitor affidavits and detailed descriptions of the records at issue.

Recent experience has demonstrated otherwise. Public bodies have refused requests for affidavit evidence, and the courts have accepted unsworn assertions without independently reviewing the records. In these circumstances, inserting an "absolutely necessary" threshold into the Act risks creating an additional barrier to meaningful review while doing little to address the existing accountability gap.

Other Canadian Jurisdictions

The landscape across Canada varies on this issue – in some jurisdictions the Commissioner can compel the production of any record for review, including records where there has been a claim of solicitor-client privilege, while others are in a similar circumstance as ours.

At the federal level, the [Access to Information Act](#) was amended several years ago to expressly authorize the Information Commissioner to examine records withheld on the basis of solicitor-client privilege during an investigation, without imposing an additional threshold of “absolutely necessary.”

To our knowledge, no issues have arisen as a result of that amendment. This demonstrates that it is possible to provide clear statutory authority for independent review of solicitor-client privilege claims while maintaining the protection of the privilege itself. It also illustrates that

meaningful oversight can be achieved without imposing additional threshold language that may impede effective review.

Recommendation

Recommendation 2026-2: Amend section 97(1) by adding after (d) a specific provision with effect similar to section 36(2.1) of the federal **Access to Information Act**.

Settlement Privilege

We disagree with Chair Orsborn's recommendation to include settlement privilege within section 30(2). Our general position regarding settlement privilege was outlined in our [supplementary submission](#) to Chair Orsborn.

Section 30(2) as it currently stands protects solicitor-client privileged information and litigation privileged information "of" a third party. Settlement privilege has been recommended to be added to this list. The difficulty is that typically what is often the subject of questions related to settlement privilege is an agreement between a public body and a third party. While it is usually clearly demonstrable as to what information is the solicitor-client privileged information or settlement privileged information "of" a third party, it is anticipated that inclusion of settlement privilege in this exception will create confusion as to what portion of the information belongs to, or is "of", the third party versus "of" the public body.

While we do have jurisprudence from the Court of Appeal about the meaning of "of" in a commercial context (see [Newfoundland and Labrador \(Information and Privacy Commissioner\) v. Beverage Industry Association of Newfoundland and Labrador, 2023 NLCA 2](#)), we will be starting from scratch in this particular context, which creates uncertainty and invites protracted and expensive legal proceedings.

Although he made this recommendation, Chair Orsborn certainly acknowledged that in past reports the Commissioner has applied section 35 to prevent the disclosure of information relating to a settlement between a public body and a third party that could harm the public body. Even if the information is, let's say, a settlement proposal from a third party, disclosure

of such a proposal could also be captured by section 35(1)(g) because it is in the financial interests of the government that such proposals and communications be protected. Whether the final agreement and related details are disclosed should be a matter of assessing the harm from disclosure as contemplated in section 35.

Chair Orsborn did not have the benefit of the most recent jurisprudence in the matter when he issued his Report. As recently as the decision in [St. John's \(City\) v. Newfoundland and Labrador \(Information and Privacy Commissioner\), 2024 NLSC 40](#), the Court has recognized that the approach taken by Commissioners, interpreting ATIPPA, 2015 as it exists, strikes the appropriate balance.

Creating a category-based exception in 30(2) rather than relying on the existing harms-based exception in section 35 not only introduces uncertainty, it would result in information being withheld from the public without having to demonstrate harm. Despite the fact that there has been lobbying for an amendment from some parties to include settlement privilege, the fact of the matter is that settlement privilege has never been listed as an exception in ATIPPA, 2015, and no one has been able to point to any scenarios where information was disclosed that has harmed any party's ability to conclude settlements with public bodies.

Recommendation

Recommendation 2026-3: No amendment of ATIPPA, 2015 to insert a settlement privilege exception.

Workplace Investigations

OIPC presented a lengthy submission on section 33 to the ATIPPA Statutory Review Committee 2020. As no statutory amendments followed that review, and as the circumstances have not materially changed, our views have remained substantially the same.

For over 10 years section 33 has been a challenge for public bodies and access to information applicants, as well as for those other parties to a workplace investigation whose information has been accessed through this unique provision. It has also been a challenge for this Office

in overseeing compliance. We have created a [guidance document](#), which has been updated to reflect jurisprudence, and while our Office has issued numerous reports pertaining to this section, it remains difficult to apply, contentious, and ambiguous.

Although the recommendations we make below may be viewed, on balance, as representing restrictions on the right of access, it is important to recognize that as stewards of the Act, we have an equal role, as recognized in section 3(2)(f) of the Act, in promoting both access to information and protection of privacy. This submission on section 33 is our effort to help find the appropriate balance between those competing values.

The essence of this section, which is unique in Canada, is that it first creates a mandatory exception to access for “all relevant information” connected to a workplace investigation. It then creates a mandatory right of access to that same information, for a party to that workplace investigation. Both are powerful clauses: like all mandatory exceptions to access, section 33 is not subject to discretion by the public body nor to the public interest override in section 9. As for the right to access, this is also extremely powerful. It applies broadly: it is not limited in time, and thus all records that are relevant to the investigation become responsive to an access request the minute they are created, regardless of the status of the investigation. It is broad in scope as well, covering all relevant documents, with no limitation to categories of documents, and with no protections for the privacy of witnesses or complainants. As we will discuss below, a major issue has been whether section 33 overrides all other exceptions to access in the Act.

We believe that section 33 as currently drafted created a number of likely unintended consequences. We therefore have three recommendations, which will be discussed in turn below.

Previous Interpretations

Despite the fact that this provision first appeared in ATIPPA in 2012, it was not until 2016 that OIPC was called upon to interpret it in a formal Report. Since then, it has appeared frequently, having been addressed or discussed in eighteen Reports, including the most recent ones:

[A-2025-005](#) – Department of Fisheries, Forestry and Agriculture;

[A-2025-021](#) – Town of Torbay; and

[A-2025-034](#) - Royal Newfoundland Constabulary.

Beginning in 2018, the Newfoundland and Labrador Supreme Court has issued decisions involving section 33, some involving appeals of OIPC reports, and others brought directly by parties. A number of those decisions have significantly changed the interpretation of section 33. The main decisions are as follows:

[Corner Brook \(City\) v. Newfoundland and Labrador \(Information and Privacy Commissioner\), 2020 NLSC 37;](#)

[Oleynik v. Memorial University of Newfoundland and Labrador, 2021 NLSC 51;](#)

[Oleynik v. Memorial University of Newfoundland and Labrador, 2021 NLSC 52;](#)

[Kirby v. Chaulk, 2021 NLSC 86;](#)

[College of the North Atlantic \(Re\), 2021 NLSC 120;](#)

[Lewisporte \(Town\) v. Newfoundland and Labrador \(Information and Privacy Commissioner\) 2022 NLSC 130;](#) and

[Kelland v. Royal Newfoundland Constabulary, 2024 NLSC 142](#) (Ongoing Matter).

Report [A-2023-021](#) (City of Mount Pearl) offers a particularly good summary, in paragraphs 58 to 65, of our developing and ongoing concerns as a result of the interpretation of section 33:

[58] In the present case, we have determined that following the College of the North Atlantic and Lewisporte decisions, the application of the different factors to be considered under section 40(5) leads us to conclude that the disclosure of almost all of the information in the investigation report would be an unreasonable invasion of the privacy of one or more individuals. Once that information is redacted, all that would remain would be isolated, meaningless fragments. We therefore agree with the decision of the City of Mount Pearl to withhold the entire responsive record from the Complainant.

[59] In some previous cases that have come before this Office, applying the interpretation set out by the College of the North Atlantic and Lewisporte decisions has in fact resulted in the disclosure of a great deal of information. By contrast, in the present case, the result has been that section 33(3) has been rendered essentially meaningless. The different treatment of the workplace investigation in the present case, and that in Lewisporte can only be explained by differences in how the two reports

were drafted, with the structure and format of the report in Lewisporte allowing the Town to redact sufficient personal information while leaving the remainder of the report intelligible.

- [60] It is absurd and troubling that the consistent application of an interpretation of the statute should lead to such inconsistent results. This case illustrates the paradoxical situation in which we find ourselves at this moment. Clearly, it was the intent of the legislature in 2012 to create a mandatory right of access for the parties to a workplace investigation but a mandatory exception for everyone else. But, following the decisions referenced here, section 33 has proven to operate only partially or, as in this instance, not at all. The intended right of access within section 33 has been entirely overridden by the privacy provisions, because the Act does not provide a guide on how to resolve the interplay between sections 33 and 40, beyond the generic balancing provision within section 40(5) that applies to all forms of personal information.
- [61] Section 40(2)(d) provides that a disclosure is not unreasonable “where an Act or regulation of the province or of Canada authorizes the disclosure.” It might be concluded that section 33 itself is a provision of an Act that clearly authorizes disclosure to the parties, and therefore such a disclosure would be deemed to be not unreasonable.
- [62] There have been a number of cases, involving both access and privacy matters, in which a disclosure has been determined not to be an unreasonable invasion of privacy (or a privacy breach under Part III) because another Act has authorized or mandated the disclosure. An example is our Report A-2021-028, in which we determined that because the Municipalities Act requires certain information to be publicly available, the disclosure of that information in response to an access request is not an unreasonable invasion of privacy.
- [63] It is tempting to conclude that such an interpretation could resolve the conflict between section 33 and section 40 and permit section 33 to operate in the way in which it was apparently intended. However, it does not appear that any of the courts referred to above considered this possibility, and there was no discussion of this point in any of the court’s decisions. Under the circumstances we are unwilling to adopt a conclusion that departs so significantly from the interpretation chosen by the court, without having placed the issue before the court in a case that permits a full examination.
- [64] The result in the present case will be particularly disheartening to the workplace complainant who, at the time that he embarked on the process of making the complaint, felt assured that he would have the right to obtain the entire results of the investigation under the then-accepted interpretation of section 33 the Act.
- [65] These unsatisfactory results highlight the flaws in the relationship between two different provisions of the Act. The courts have endeavoured

to reconcile the apparent conflict, but the courts can only interpret the statute as it is written. Legislative intervention will likely be necessary to clarify the interpretation issues and resolve the conflict.

Clarify the Paramountcy of Section 33

If our understanding of the purpose of section 33 is correct, namely, that it was intended to provide parties to a workplace investigation with a greater right of access than existed before the provision was enacted, then section 33 must be interpreted as overriding section 40. Otherwise, where information relating to the applicant also constitutes the personal information of another individual, section 40 could operate to restrict access to the applicant. This would defeat the purpose of section 33, as the ordinary right of access to one's own personal information would already provide the applicant with the information to which they are entitled, thus rendering section 33 redundant.

However, there is no specific reference in the statute that would identify either section 40 or any other exceptions as the sections to be overridden. Logically, therefore, as presently written, section 33 must be interpreted to override all exceptions in the Act, or none of them. If section 40 was a discretionary exception, then perhaps a logic might be considered whereby the class of discretionary exceptions could be overridden, but not the mandatory exceptions; but this is not the case. This leaves us in a precarious and uncertain place, as there are certain exceptions which perhaps, in our view, should prevail over section 33.

In addition, we are of the view that section 33 should be subject to the public interest override provision in section 9. In circumstances where high-level public officials are involved in perpetrating serious workplace harassment, there can be a public interest in a certain amount of transparency in order to facilitate appropriate accountability.

This Office would therefore recommend that section 33 be amended to provide that certain other exceptions in the Act are to be applied to the records before any disclosure, regardless of section 33. Chief among those would be:

- section 27 (cabinet confidences);
- section 30 (legal advice);

- section 31 (disclosure harmful to law enforcement);
- section 37 (disclosure harmful to individual or public safety); and
- section 41(c) (disclosure of House of Assembly service and statutory office records).

Additionally, amend section 33 to ensure that the exceptions to be applied are subject to a consideration of whether the public interest favours disclosure. The following is our suggested wording for the addition of subsections to section 33:

- (5) Notwithstanding subsections (3) or (4), the head of the public body shall disclose only the information that remains after the application of the exceptions to access in sections ...
- (6) provided, however, that the discretionary exceptions referred to in subsection (5) shall not apply where it is clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception.

Limit the Temporal Scope

Section 33 is intended to provide the parties to a workplace investigation with an equal right to information. However, because the parties to a workplace investigation are usually not equal, the disclosure required by section 33 could harm individuals as well as negatively impacting the process itself.

Section 33 is intended to apply primarily to investigations of harassment in the workplace. Harassment is defined in section 33, and that definition is similar to those found in other statutes and in numerous harassment or respectful workplace policies, both of public bodies and private sector employers.

What section 33 does not reflect is that harassment typically involves a power relationship between the perpetrator or abuser and the subordinate victim. Harassment is only possible because of that inequality. The power relationship also means that harassment is easily accompanied by intimidation of the victim, and a complaint can easily result in retaliation. It is only because of that inequality that specific respectful workplace policies, and specific workplace investigation processes, are necessary.

Most of the examples of workplace investigations we have seen involve the appointment of independent third party investigators. Our comments below are oriented towards that scenario. There are, in Canada, a number of practitioners who specialize in workplace investigations, and there is a professional literature on the conduct of such investigations. In that literature, and in many respectful workplace policies, it is recognized that because of the inequality in power relationships, harassment complainants and witnesses need assurances of confidentiality. Otherwise, the fear of intimidation and retaliation will prevent them from coming forward. The investigator needs to be able to provide assurances of confidentiality in order to build a relationship of trust with the complainant and witnesses, and to ensure complete disclosure during the investigatory process.

Part of the challenge with section 33 is that those who file workplace complaints and those who investigate those complaints do not necessarily have a clear understanding of its implications, and public bodies that create the policies and procedures for such processes have usually also not done so with section 33 in mind. Specifically, promises of confidentiality that exist in policy may have been made, not only absent consideration of section 33, but absent consideration of access to information rights under ATIPPA, 2015 generally.

Therefore, the investigator should have control of the information collected during the course of the investigation and should have the discretion to decide what information is provided to the alleged perpetrator, in how much detail, and at what stage in the investigation. Complainants and witnesses have the right to be told from the very beginning what the limits on confidentiality may be, whether or at what stage their identities may be disclosed, and whether their exact words and other personal information will be disclosed to the perpetrator, or only summaries of their statements.

In typical investigations, the investigator has a mandate to provide a report to the employer containing a statement of facts, summarizing the information provided by witnesses, without any recommendation for action. Witness statements may or may not be provided to the employer, or to the respondent, and may be summarized, de-identified or redacted. All of these considerations should, ideally, be reflected in policies and procedures. The reality,

however, is that there is a broad range of resources and expertise between the smallest municipality and the largest government department, so this may not always be the case.

The employer may choose from a range of possible actions upon receipt of a report, and the choice will affect ongoing workplace relationships. The complaint may be determined to be unfounded. For some kinds of harassment, an informal resolution, respectful workplace training, or a mediation process may be possible. Sometimes a finding may justify separating the parties in the workplace, or discipline, or even termination of employment. Some of those possible resolutions are not necessarily adversarial and may not even require the identification of the complainant or of witnesses to the respondent, much less require detailed statements to be provided. In some cases, the respondent may not ever know that there was an investigation.

In many circumstances disclosure of the identities of witnesses, or the details of their statements, can have extremely harmful effects. Disclosure makes it possible for the perpetrator to intimidate the victim or the witnesses, to prevent them from confirming their statements at a later stage, or in another proceeding. It also makes it possible for the perpetrator to retaliate against the complainant or witnesses, even outside the workplace. Perhaps worst of all, in circumstances where the complainant and witnesses were promised and expected confidentiality, disclosure will have the effect of poisoning the workplace and nullifying any potentially positive results of the harassment investigation. Just as the right to refuse unsafe work is difficult for employees to assert outside of unionized workplaces, the right to make a harassment complaint will seldom be exercised in a workplace where it is known that confidentiality will not be preserved and retaliation is possible.

It may be argued that a respondent is entitled to the records covered by section 33 to make a “full answer and defense” to the allegations. However, in our view, this argument misunderstands the nature of the investigative process.

The legal right to full disclosure of evidence, and the identity of an accuser, exists in relation to an adjudicative process in which there can be a binding decision affecting a respondent’s legal rights. A workplace investigation is not an adjudicative process. It is analogous to a police

investigation that might lead to criminal charges, or an employer's investigation into misconduct that could lead to discipline. At the investigation stage, policy or practice often dictates that a respondent must be notified of an investigation, but there is no legal requirement that this be done, much less to engage the respondent to participate. ATIPPA, 2015 recognizes this distinction, for example, in section 5(1)(k), in which the Act does not apply to law enforcement records where the investigation has not been completed.

It is of course true that some workplace harassment investigation policies provide that the respondent is to be notified of the complaint and asked for a response. Some policies require that the respondent be interviewed. These provisions, however, are policy decisions, not legal rights, and in the absence of a request for access by the respondent which would bring section 33 into play, it remains the prerogative of the investigator to decide when and how much the respondent is told. It is our experience that workplace complainants and witnesses feel betrayed by disclosures made under section 33, and also that respondents in harassment complaints are usually the parties who will make access requests under that section.

One solution that might be proposed by some would be to repeal section 33 altogether, leaving public bodies to rely on the various exceptions, particularly section 40. Parties to a workplace investigation would be without the special rights set out in section 33, but each individual would retain their ability to request access to their own personal information. This creates its own set of problems, however (or rather, returns us to the original ones which resulted in the creation of this provision in the first place). Furthermore, it does not solve many of the problems created by section 33. As noted above, this was the situation prior to the introduction of section 33, and it created substantial difficulties when an access request was filed, which involved teasing out the personal information of the parties from the various statements and other records, and redacting accordingly. Respondents will still be able to obtain a majority of the information in statements of complainants and witnesses about them, so the same workplace dynamics will remain at play.

Therefore, we recommend that Government amend section 33 to provide that disclosures of workplace investigation records in response to an access request are only to be made after the workplace investigation has been completed, or anytime thereafter, including before any

resulting discipline is imposed or corrective action is taken by the employer. This would permit the investigator to retain control of the investigation, to explain any limits on confidentiality to witnesses, and to control when, and in what detail, the respondent is given information during the investigation process. It would also prevent a party from disrupting the investigation with an access request while the investigation is ongoing. It would furthermore assist the investigator or the public body (or OIPC in a complaint investigation) in determining “relevance” after the investigation is complete. Furthermore, in accordance with records retention and destruction policies that may be approved under the appropriate statute or bylaws, if a complaint is withdrawn before completion, a public body could create a policy to destroy any records created or gathered by the investigator. Moreover, records of statements provided orally or in writing by a witness or complainant, or the identity of same, could be withheld until the conclusion of the investigation, unless explicit consent to disclosure is given by the individual. All parties could retain the right of access to their own statements at any time. If a temporal limitation was placed on the right of access as proposed, it would also allow for the appropriate and legally authorized destruction of any transitory records prior to an access request being allowed, such as investigators’ notes or audio recordings.

Expand the Scope of Employment Relationship

One issue that has become apparent with section 33(1)(c) is that it is limited to the employment context; however, it is not entirely obvious that this should make a difference. While a harassment investigation undertaken regarding the actions of a member of a Board of Directors for a public body is not a workplace investigation, it is still a harassment investigation within the public sector context and within a public body.

It is not entirely clear why the parties to such a harassment investigation would have different rights to access than those involved in a workplace investigation. If section 33 was expanded to include harassment investigations in such contexts, then care should be taken to ensure that the way it overrides other exceptions to access operates correctly.

Recommendations

Recommendation 2026-4-1: Clarify the paramountcy of section 33 with amendments:

- indicating that certain other exceptions in the Act are to be applied to the records before any disclosure, regardless of section 33; and
- ensuring that the exceptions to be applied are subject to a consideration of whether the public interest favours disclosure.

Recommendation 2026-4-2: Amend section 33 to limit disclosure of records relating to a workplace investigation such that the right of access would commence after a workplace investigation has been completed. For clarity, disciplinary decisions need not be finalized or imposed for the right of access to commence and the right of access would be enduring thereafter.

Recommendation 2026-4-3: Consult with public bodies on whether section 33 should be broadened to apply to harassment investigations beyond the employment context.

Third Party Business Interests

The current framework established by sections 19 and 39 of ATIPPA, 2015 is functioning effectively and strikes an appropriate balance between transparency and the protection of third-party business interests and therefore should be maintained.

The substantial body of case law in this province that has been developed over the past decade or more, together with numerous reports and guidance documents issued by this Office, has significantly reduced the confusion and uncertainty that characterized the early application of section 39. We now have jurisprudence from our Court of Appeal such as [Newfoundland and Labrador \(Information and Privacy Commissioner\) v. Beverage Industry Association of Newfoundland and Labrador, 2023 NLCA 2](#) and [Corporate Express Canada Inc. v. Memorial University of Newfoundland, 2015 NLCA 52](#).

There have been times in the past when complaints relating to third party business records were a major focus of the investigations division of this Office, and there were often multiple matters moving through the courts as well. This has, by and large, come to a halt. In our view,

this means that the interpretation issues experienced earlier have been resolved. It is resulting in fewer complaints because public bodies know how to apply section 39, and there is a body of case law and guidance available to assist third parties and applicants.

We do not believe that there is a compelling basis to alter a framework that has been carefully developed through the efforts of former Chief Justice Wells and his committee and refined through judicial interpretation. It is our opinion that introducing amendments that impact section 19 or 39 of ATIPPA, 2015 will remove the clarity that has been established, and result in more complaints and court applications, meaning that applicants, third parties, and public bodies will have to devote and expend additional and unnecessary resources attempting to resolve issues that are now reasonably well settled.

Current Legislative Structure

The current structure of section 39 and the notification process in section 19 are the product of deliberate reforms arising from the 2014 ATIPPA Review. The review restored the three-part harms test for third party business information, a model widely used across Canada and shared by jurisdictions such as Alberta, British Columbia, and Ontario. As a result, there is extensive jurisprudence interpreting and applying this exception.

The 2014 ATIPPA Review also established the current notification regime in section 19. Notification occurs only after a public body has formed an intention to release information that may be subject to section 39. Third parties are then provided with an opportunity to appeal, and disclosure is suspended until all appeal rights have been exhausted. This framework was intentionally chosen over broader notification models that require notification whenever disclosure is merely being considered, which typically result in needless alarm on the part of third parties, resulting in unnecessary complaints and substantial delays.

Public Procurement Act

Section 8(2) of the [Public Procurement Regulations](#) has assisted in the reduction of third-party complaints to this Office as well as helped manage the expectations of businesses participating in the procurement process. It has also been very beneficial to public bodies in

assessing what information it can disclose to requesters and what information it needs to review more closely in relation to section 39. Section 8(2) of the Regulations state as follows:

8. (2) A bid received in response to an open call for bids shall identify any information in the bid that may qualify for an exemption from disclosure under subsection 39(1) of the *Access to Information and Protection of Privacy Act, 2015*.

This section of the Regulations puts the onus on third parties to identify information that may qualify for an exemption from disclosure under subsection 39(1) of ATIPPA, 2015. This helps public bodies determine if a section 19 notification is required when processing an access request. If the third party has not identified any information that they believe would qualify for exemption from disclosure under section 39 of ATIPPA, 2015 then the public body should be able to proceed to release that information after they have reviewed the information to confirm there are no other considerations necessary. Our view is that section 8(2) has helped provide public bodies with more certainty when deciding to release or withhold third party business information as well as helped reduce the number of complaints to OIPC by third party complainants.

While the Public Procurement Regulations came into force in 2018, it took some time for public bodies and third parties to get used to how it worked, so the benefit of those Regulations was perhaps not fully realized at the time of the 2020 ATIPPA Statutory Review. Since then, however, it has become clear that the current statutory regime is clear, user-friendly, and understandable to all parties.

ATIPP Office Statistics and OIPC Reports

Based on the statistics published in the ATIPP Office's Annual Reports, the use of section 39 as an exception claimed by public bodies has been declining and the statistics also show that section 39 makes up a small percentage of the total exceptions claimed in general requests to departments and public bodies. The following table focuses on section 39 claims over the last 5 years and was created from the "General Requests – Exceptions to Disclosure for General Requests by Departments and Public Bodies" that the ATIPP Office publishes in its Annual Reports.

ATIPP Office Annual Report	Number of Times Section 39 Claimed	Section 39 Percentage of Total Exceptions Claimed
2020-2021 , Table 5b	148	8%
2021-2022 , Table 5b	115	4%
2022-2023 , Table 4b	62	2%
2023-2024 , Table 4b	60	2%
2024-2025 , Table 4b	93	3%

Our Office has also experienced a decline in reports involving section 39. We have observed a decline in reports involving third party complainants (this would be where the public body intends to disclose the records, issues a section 19 notification and the third party makes a complaint to OIPC) as well as a reduction in the number of reports where public bodies claimed section 39 to withhold the records which resulted in a complaint (this would be where the public body relied on section 39 to withhold the records and the access requester makes a complaint to OIPC).

The following is a table derived from OIPC Commissioner Reports from 2020 to 2026 to give a general overview of the number of reports that involved a claim of section 39 as an exception by public bodies as well as which parties are making the complaints to our Office.

Year	OIPC Reports Involving Section 39	Third Party Complainants (PB Intends to Release and Third Party Makes Complaint)	Complainants (PB Withholds and Initial Access Requester Makes Complaint)
2020	9	6	3
2021	7	2	5
2022	5	1	4
2023	2	1	1
2024	1	0	1
2025	2	0	2
2026 (to Sept 29)	3	0	3
Total	29	10	19

ATIPPA Statutory Review Committee 2020 Recommendations - OIPC Disagrees

We disagree with some of the recommendations from the ATIPPA Statutory Review Committee 2020 relating to section 39. We believe that amendments from those recommendations could undermine the carefully balanced framework that has evolved in Newfoundland and Labrador through the operation of sections 19 and 39 of ATIPPA, 2015.

The recommendations that we disagree with are as follows.

Chair Orsborn Recommendation: That the Act be amended to: Remove the requirement that information has to have been supplied in confidence from the exception for disclosure harmful to third parties' business interests. [Appendix K, s. 39]

Our Office disagrees with this recommendation, and we provided detailed commentary in a letter dated March 4, 2021, on this issue in [OIPC Comments in Response to Hypothetical Amendment to Section 39](#) beginning at page 2. OIPC's position was, and remains, that the "supplied in confidence" requirement in the three-part test in section 39 of ATIPPA, 2015 is an essential component of that provision and should not be removed.

The "supplied" requirement is intended to protect immutable information, meaning information provided by a third party that exists independently of, and is not subject to, negotiation. By contrast, negotiated information, such as prices, quantities, specifications, and other contract terms, is the product of an agreement between the parties. Even if no actual negotiation occurs (i.e. an offer is made and accepted with no further discussion), this can be considered a contract between two parties and is the product of both parties.

Information that forms part of a negotiated agreement should be disclosed so that the public can scrutinize how much a public body is paying, to whom, and for what purpose. As a result, information contained in contracts will often fail to meet the "supplied" requirement because it forms part of the negotiated terms of the agreement. While disclosure of contract terms may sometimes affect confidentiality or increase competition, those consequences are an inherent aspect of doing business with public bodies, which must operate through open and transparent procurement and contracting processes.

In OIPC's view, the "supplied" component is fundamental to section 39. It provides a clear distinction between negotiated contract terms, which are generally subject to disclosure, and third-party information that may warrant protection. It serves as a clear and well-established threshold supported by decades of Canadian jurisprudence. This proven framework promotes consistency in decision making, facilitates the informal resolution of complaints, and reduces complaints, and court appeals.

Removing this requirement, or reducing the test, would weaken the public right of access, reduce legal certainty, and depart from the established Canadian approach to balancing transparency with the protection of legitimate third-party business interests.

OIPC recommends retaining the “supplied in confidence” requirement and strongly believes that it preserves both predictability and efficiency of section 39 while continuing to protect third party interest.

Chair Orsborn Recommendation: That the Act be amended to: Provide a mandatory exception for trade secrets. [Appendix K, s. 39(1)(a)]

Our Office disagrees with this recommendation, and we provided detailed commentary on this issue in [OIPC Comments in Response to Hypothetical Amendment to Section 39](#) beginning at page 4. OIPC's position was and remains that trade secrets are already adequately protected under section 39 of ATIPPA, 2015, and therefore a separate exception is unnecessary.

Based on OIPC's experience, it is extremely rare for trade secrets to be disclosed to public bodies in the first place, making it unlikely that such information would become responsive to an access to information request. Further, public bodies generally take a cautious approach when assessing third party business information, and section 39 provides protection for genuinely sensitive commercial information where the statutory requirements are met.

Chair Orsborn Recommendation: That the Act be amended to: Allow public bodies to consult with third parties while considering requests for information the release of which might be harmful to their interests. [Appendix K, s. 19(1)]

Our Office disagrees with this recommendation. Public bodies have strict timelines under ATIPPA, 2015 for responding to an access request and notification to a third party under section 19 does not suspend the timeline under section 16 of ATIPPA, 2015 for responding to an access request. Adding in a consultation with the third parties will provide procedural challenges for public bodies. While we appreciate that informal consultations do happen between public bodies and third parties; having a legislative amendment would create an expectation on the part of third parties for every request and would certainly complicate the matter, often unnecessarily.

In our view, public bodies have two clear paths involving section 39 where consultation with the third party is not necessary.

- Where a public body determines that section 39 applies, it must refuse disclosure.
- Where a public body determines that section 39 does not apply, it must disclose the information.

Notification is only triggered where the head of the public body intends to disclose information and has reason to believe that the information "might be excepted from disclosure." Notification is only required in the intermediate circumstances and section 19 sets out a path for notification and consultation with the third party at this stage.

Public bodies have proven that they can assess access requests and the potential applicability of section 39 without the need for additional consultation with third parties. Should uncertainty exist regarding the exception then public bodies have a route to consult the third party at that time through formal notification.

There is also a risk associated with permitting public bodies to consult with third parties while they are still assessing an access request. Under ATIPPA, 2015, it is the public body that is responsible for determining whether the requirements of section 39 have been met. Allowing

consultation at this early stage risks shifting that responsibility to third parties whose interests may not align with the public body's statutory obligations. Third parties may seek to influence the outcome, potentially undermining the public body's independent assessment of both the records at issue and the application of section 39. In some cases, public bodies may be inclined to defer to the third party's recommendations rather than undertake their own analysis. The responsibility of applying the Act is on public bodies, not third parties.

For these reasons, we see no benefit to allowing public bodies to consult with third parties while the public body is considering the request.

Chair Orsborn Recommendation: 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. [Appendix K, s. 44(1.1)]

Our Office disagrees with this recommendation. If a public body refuses access to information claiming that section 39 applies, the access requester can make a complaint to OIPC for a review of the public body's decision. In this situation the parties are clear, the public body and the access requester.

Where a public body decides to withhold information under section 39, it must be satisfied that the evidence supports the three-part test set out in that section. If the public body has already determined that section 39 applies and has refused access on that basis, we see no value in making the third party a party in our complaint process, as the information has already been withheld through the public body's refusal decision.

If an access requester makes a complaint to OIPC the determination that must be made is whether the public body applied section 39 appropriately, not whether the third party agrees with the public body's decision.

Making the third party a party to the complaint process would also introduce a significant degree of duplication. The public body would continue to bear the burden of explaining and defending its decision under the Act, while the third party would likely make many of the same

arguments in support of withholding the information. This would add complexity to the process without meaningfully assisting in reaching a resolution.

In addition, granting third parties party status to the complaint would create procedural and administrative challenges. Our Office operates within legislated timelines and only has 65 business days to complete a report where one is required. Adding another party would inevitably increase the volume of submissions, correspondence, and procedural steps associated with OIPC's review. In some cases, there may be multiple affected third parties, each potentially entitled to participate and make separate representations. This could significantly lengthen the review process and impede the timely resolution of complaints.

In our view, there is also a risk associated with adding third parties as parties to the complaint process: it could shift responsibility for section 39 decisions away from public bodies. We have already observed situations where a public body has completed its analysis and reached a definitive conclusion that section 39 does not apply, meaning that the records should be disclosed. However, the public body nonetheless issues a section 19 notification. This may occur out of an abundance of caution or a desire to avoid conflict with, or maintain a positive relationship with, the third party, especially in business relationships. That approach is inconsistent with the purpose of the notification provision, and our Office has commented on this practice in previous reports.

Public bodies are responsible for determining whether the requirements of section 39 have been met and that responsibility should not be diluted by making third parties' participants in complaints involving section 39. There is a risk that public bodies may become less rigorous in conducting their analysis, relying instead on the expectation that the third party will defend its interests if a complaint is made. Over time, this could weaken the public body's accountability for its access to information decisions and undermine the fact that the public body, not the third party, is the decision maker under the Act.

For these reasons, we see no compelling benefit to adding third parties as parties to the complaint process where information has already been withheld by the public body under section 39.

ATIPPA Statutory Review Committee 2020 Recommendations - OIPC Agrees

In our view, three of the recommendations from the ATIPPA Statutory Review Committee 2020 relating to section 39 of ATIPPA, 2015 would not affect or impair the effectiveness or functioning of section 39 to the same extent as other recommendations relating to section 39 would. These recommendations are:

- that the Act be amended to: Provide a 20-year sunset clause on third-party business information. [Appendix K, s. 39(4)];
- that the Act be amended to: Make the exception for disclosure harmful to third parties' business interests subject to the public interest override. [Appendix K, s. 9(2)];
- 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. [Appendix K, s. 19(5)(c)].

We have no concern with an amendment providing a 20-year sunset clause on third party business information nor do we have any concern with an amendment requiring a third party who files a complaint or appeal to provide a copy of the complaint or notice of appeal to the public body, in fact both of these recommendations are positive.

The more substantive of the above recommendations is the proposal to make section 39 subject to the public interest override in section 9. The threshold for applying the public interest override is high, and OIPC cannot confirm whether it has ever been used by a public body. If it had been used, it would have resulted in a public body disclosing information to an applicant despite the information otherwise qualifying as an exception to access. In such circumstances, a complaint to OIPC would be unlikely, as the applicant would have received the information sought. Consequently, OIPC may not have been aware of any instance in which the public interest override was used.

The only instance in which the court has agreed that section 9 applies is in [Asphalt Product Industries Inc. v. Town Council of Come by Chance \(Town\), 2023 NLSC 12](#). In that case, the court's analysis concluded with a finding that sections 35 and 39 did not apply to the information at issue, and therefore the information was to be disclosed.

However, a further finding was also made in which Justice Browne stated that even if he were wrong, the public interest override would apply to require the information to be released. Paragraph 89 stated:

Having previously reviewed the sealed tax agreements and determined they are appropriate for the Town to disclose under either section 39(1)(a)(ii) or 35(1)(f), I find Asphalt Product has discharged its onus under section 9 by establishing that there is a sufficient public interest in disclosure of the tax agreements that outweighs the statutory exceptions relied upon by the Town.

While Justice Browne concluded that the public interest override would apply if he were incorrect in his interpretation, the issue was ultimately academic because sections 35 and 39 had already been determined not to apply and therefore the records should be disclosed. Furthermore, section 35 as a discretionary exception to disclosure is already subject to the public interest override in section 9 whereas the practical interaction between section 39 and the public interest override in section 9 was never fully considered or adjudicated.

Chair Orsborn's conclusion at page 193 of the [ATIPPA Statutory Review 2020 Report](#) was:

As discussed in the section of this report addressing s. 9, I consider it appropriate, notwithstanding the mandatory nature of the exception, to make the exception subject to the s. 9 public interest override.

Chair Orsborn provided a hypothetical scenario involving the addition of a public interest override in section 39 which would be "section 39(4)". Our Office provided detailed commentary on this issue in [OIPC Comments in Response to Hypothetical Amendment to Section 39](#), stating in part:

Furthermore, and most importantly, the hypothetical section 39(4) is unlikely to be used. For one, our experience is that when public bodies find that a discretionary exception applies, they claim it. Whether or not the claim is valid is the matter under consideration upon review by the OIPC or in a Court Appeal, rather than the exercise of discretion. To convert section 39 into a discretionary exception under the conditions outlined in section 39(4) is unlikely to result in greater transparency to any significant degree. Even section 9 itself is a very high threshold, however it at least has the advantage that once the threshold is met, the exception no longer applies. Functionally, the hypothetical section 39 cannot be considered to be an "over-ride" provision because it does not actually over-ride the exception. It merely inserts an additional decision point where the public body has an opportunity to exercise discretion. Based on what

we have heard and what we know from our experience with public bodies, there is a strong orientation towards maintaining positive working relationships with third parties, which we believe would certainly militate against a public body exercising its discretion to disclose information to which the exception has been found to apply. An alternative may simply be to list section 39 in section 9(2).

While we support making section 39 subject to the public interest override, we note that the practical operation of section 39, as a mandatory exception, within the framework of section 9 has not been thoroughly examined. We do not support section 39 being changed to a discretionary exception therefore careful consideration should be given to how such an approach would function in practice and how the mandatory nature of section 39 would interact with the exercise of the public interest override.

Recommendations

Recommendation 2026-5-1: No amendment to the operation of sections 19 and 39 and maintain these sections as they are.

Recommendation 2026-5-2: Amend the Act to provide a 20-year sunset clause on third party business information.

Recommendation 2026-5-3: 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.

Recommendation 2026-5-4: Amend the Act to make the exception for disclosure harmful to third parties' business interests subject to the public interest override.

Public Interest Override

The historical context of public interest override can be reviewed in our [2020 submission](#) beginning at page 40 in that document. We agree with the recommendation that the public interest override be expanded to other exceptions as indicated by Chair Orsborn. Beyond that, we note that there has been further judicial consideration of the public interest override in [Asphalt Product Industries Inc. v. Town Council of Come by Chance \(Town\), 2023 NLSC 12](#). In

that matter, despite having found that the exceptions claimed by the Town (sections 35 and 39) did not apply to allow or require the information to be withheld, the Court also found that the third party had discharged its onus to establish that the public interest override also applied. In making this finding, the Court did not comment on the fact that section 39 is currently not subject to the public interest override. This aspect of the Court's ruling, though, does establish that there may be legitimate circumstances from time to time where it would be appropriate to allow the public interest to outweigh the exception in section 39, and indeed in other exceptions not currently covered by section 9.

Recommendations

Recommendation 2026-6-1: Clarify that the burden of proof in the application of the public interest override does not rest solely on the applicant or the public body but that any party, including OIPC at the review stage, is obligated to bring forward evidence that could be relevant to this determination.

Recommendation 2026-6-2: Include third party business information (section 39) among the list of exceptions to access to which the public interest override in section 9(1) applies.

Recommendation 2026-6-3: Consider amending section 9(3) to remove the potential for limitation of its applicability to matters that are "urgent" as a temporal consideration.

Information Technology Security

In the previous ATIPPA review OCIO sought a change in the current statutory language which protects information security and cybersecurity, which is found at section 31(1)(l). Chair Orsborn's report quotes at length the challenges faced by cybersecurity officials, of which we are quite aware, having in 2023 issued our [Report P-2023-001/PH-2023-002](#) into the cyber attack on the province's health care system.

Chair Orsborn ultimately recommended a new harms-based exception to be added as section 31.1, which is found in Appendix K of his Report. In our view, the provision that was proposed is unnecessarily prescriptive and expansive. Furthermore, it is arguable whether the exception

is in fact a harms-based one, because it allows a public body to withhold, at subsection 2, information which threatens the confidentiality of the province's data. Data is information. In fact, the entire purpose of ATIPPA, 2015 is to allow access to information (or data) held by public bodies, with limited and specific exceptions. While the provision defines "information technology security information" it presents the definition as a non-exhaustive list, opening the door for public bodies to attempt to broaden the definition over time.

Other jurisdictions in Canada have enacted provisions that protect cybersecurity using a harms-based exception, but they have done so without the prescriptiveness proposed by Chair Orsborn. This allows the arguments and evidence to focus on assessing the harm, rather than whether the information meets a certain description or is of a certain kind.

As a further example of this, the provision proposed by Chair Orsborn would allow a public body to withhold the name of a vendor or the name of a technology. While there are certainly circumstances under which the name of a vendor or technology must itself be protected, that will not be the case in all circumstances. Public-facing technology is commonplace today, and it allows the public to obtain services from public bodies. Public bodies contract with vendors for those services, and the names of those companies or technologies is not something that can or should be hidden from the public. If security were the only consideration, likely due to an abundance of caution, no information would ever be released relating to technology used by public bodies. In the statutory context of ATIPPA, 2015, however, the public good of transparency and accountability must be considered as well. For that reason, it is preferable to enact a simply worded harms-based exception that will best allow the appropriate balance. The following examples are illustrative.

Nova Scotia's recently amended FOIPOP at section 15(1)(k) contains this version: May refuse to disclose "if the disclosure could reasonably be expected to harm the security of any property or system, including a building, a vehicle, a computer system or a communications system."

Alberta's new **Access to Information Act** which came into force in 2025 has the following provision at section 23(1)(n) May refuse to disclose "if the disclosure could reasonably be

expected to harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.”

British Columbia’s FIPPA includes a comparable provision at section 15(1)(l): “may refuse to disclose to an applicant if the disclosure could reasonably be expected to (l)harm the security of any property or system, including a building, a vehicle, a computer system or a communications system.”

Unlike the above examples where the provision is part of a larger law enforcement exception, Manitoba’s FIPPA has a standalone provision at section 26: “The head of a public body may refuse to disclose information to an applicant if disclosure could reasonably be expected to harm or threaten the security of any property or system, including a building, a vehicle, an electronic information system or a communications system.”

The above examples are typical of what we might refer to as an “information security” exception, although they include the protection of other public body assets as well. These provisions have resulted in relatively clear jurisprudence that is useful across jurisdictions, and even in statutes that have recently been amended or completely revised, the statutory language outlined above is common across Canada. Our Office is on record, through our reports into the cyberattack on the provincial health care system and others, that we take cybersecurity very seriously, and we are certainly not arguing for a provision that could put the personal information of Newfoundlanders and Labradorians at risk. We do see the need to strike a balance, however, and clearly that is where legislatures across Canada have landed as well. A basic, simply worded harms-based exception will strike this balance, rather than an overly prescriptive version that may be outdated, given the pace at which things change, within a short period of time.

Recommendation

Recommendation 2026-7: Replace section 31(1)(l) of ATIPPA, 2015 with British Columbia’s security provision at section 15(1)(l) of FIPPA.

ACCESS TO INFORMATION PROVISIONS - TIMELINES

Terms of Reference Request: Review exceptions to access, **timelines for response**, and the effectiveness of current administrative procedures and the current cost schedule.

Access Request Timelines and Extensions

Section 16 of ATIPPA, 2015 is fundamental to the success of access to information laws in Newfoundland and Labrador. The legislative requirement that public bodies shall respond to an access request without delay and in any event not more than 20 business days after receiving it ensures that applicants can expect to receive records in a timely manner. Our 2020 submission included a jurisdictional scan of response timelines for access requests across Canada. As there have been some changes in timelines, this scan has been updated as follows.

Timelines that Have Not Changed

Jurisdiction	Section	Time Limit	Comments
Federal Access to Information Act	Section 7	30 days	Presumed to be calendar days and not business days as the term “business day” is defined and used in other sections.
Federal Privacy Act	Section 14	30 days	Presumed to be calendar days as no mention of “business day” in the Act.
New Brunswick	Section 11(1)	30 business days	
Nova Scotia	Section 7(2)	30 days	Presumed to be calendar days as no mention of “business day” in the Act.
PEI	Section 9(1)	30 days	Presumed to be calendar days as no mention of “business day” in the Act.
Québec	Section 47	20 days	Presumed to be calendar days as no mention of “business day” in the Act.

Saskatchewan	Section 7(2) The Freedom of Information and Protection of Privacy Act and Section 7(2) Local Authority Freedom of Information and Protection of Privacy Act	30 days	Presumed to be calendar days as no mention of business day in either Act.
British Columbia	Section 7(1)	30 days	Presumed to be calendar days as no mention of “business day” in the Act.
Nunavut	Section 8.(1)	25 business days	

Timelines that Have Changed

Jurisdiction	Section	Time Limit	Comments
Ontario	Section 26(1) Freedom of Information and Protection of Privacy Act and Section 19(1) Municipal Freedom of Information and Protection of Privacy Act	45 business days Previously 30 (presumed) calendar days.	This is now the longest timeframe in Canada.
Manitoba	Section 11(1)	45 days Previously 30 (presumed) calendar days.	Presumed to be calendar days as no mention of “business day” in the Act.
Alberta	Section 13(1) Access to Information Act	30 business days Previously 30 (presumed) calendar days.	Freedom of Information and Protection of Privacy Act repealed, now the Access to Information Act and Protection of Privacy Act

Yukon	Section 50(1)	30 business days Previously 30 (presumed) calendar days.	
Northwest Territories	Section 8(1)	20 business days Previously 30 (presumed) calendar days.	

While this Committee may hear from applicants who are critical about how long it takes to get records, the 20 business days set out in ATIPPA, 2015 is among the best in Canada. This Committee may also hear from public bodies advising that 20 business days is not nearly enough time, however, the legislation contemplates time extensions when they are necessary and when approved by the Commissioner. The vast majority of extensions are met with full or partial approval by this Office and subsequent approvals for extensions of time are also granted if there are difficulties retrieving records, the request consists of a large volume of records, the absence of a coordinator due to illness or personal leave, consulting third parties, or similar valid reasons.

Extension Applications Received by OIPC:

Year	Number of Extension Applications
2021-2022	604 (covid)
2022-2023	502
2023-2024	820
2024-2025	1102
2025-2026	1089

The 2024-2025 Annual Report of the ATIPP Office indicates at page 7 that the percentage of access requests being responded to within 20 business days is 76%. This is a significant portion of requests and is still the best evidence that ATIPPA, 2015 is working as intended to quickly get records into the hands of requesters without delay. OIPC's position is that no amendments to section 16 (Time Limits) and 23 (Extensions) are required.

This Office is understanding of the continuous increase in the number of extensions being sought by public bodies having risen from 502 to 1102 in only 3 years. Part of the reason for this is also the general increase in the number of access requests being made generally, but we are seeing additional days being requested for executive review in the range of 5 - 20 days. This has placed administrative burdens on both the public bodies and this Office to ensure that extensions are applied for, reviewed, decided upon, and communicated within a short time frame. The options explored by Chair Orsborn were to:

- 1) increase the number of business days that a public body has to respond to an access request;
- 2) allow a public body to self-extend timelines in defined circumstances for up to 10 days with notice to the Commissioner and the ATIPP Office; and
- 3) communicate directly with an applicant to reach consensus on an appropriate timeline with notification to the Commissioner.

Anything beyond the 20 days begins to erode the effectiveness of ATIPPA, 2015 and reduces the ability of the Act to ensure applicants receive records expeditiously. This Office opposes any amendment that allows a public body to approve its own time extensions even where they are reviewed by the head of a public body. It is essential, in our view, that the legislation set out clear time limits and that any extensions ought only be approved by OIPC. One of the issues identified by coordinators in the past is that extension applications take procedural time that could best be spent on the actual access request. If a new process still requires an ATIPP Coordinator to adhere to internal processes to do the same thing as applying to OIPC to justify the extension, then really there is little change, and we have lost independent oversight for nothing.

Lastly, this Office cannot agree to any option where an applicant must decide if an extension is warranted. It places an applicant in an untenable situation. Most applicants are not experts or sophisticated in how ATIPP processes work, how access requests are completed, what redactions are justified by the Act, or how long any of these processes should take. To have a public body negotiate extension timelines with an applicant, in most circumstances, is not appropriate as the two parties are not on a level playing field. The public body clearly has the

advantage of experience and could convince an applicant into an extension they don't understand or even want. From an applicant's perspective, the public body holds the records and decides what records the applicant will receive. While some sophisticated applicants will understand that ATIPPA, 2015 is a rights-based statute, many may feel that they have no choice but to go along with the proposed extension, not wanting to get on the public body's "bad side" and hoping to get records eventually.

Allowing a public body to either self-extend or to negotiate an extension with the applicant also undermines a key benefit of the extension process. Having to go to the Commissioner to apply for an extension makes it clear to both applicants and public bodies that there is independent oversight that can prevent unnecessary and overly lengthy extensions, while factoring in the challenging, time-consuming work required to complete a request. The core rationale for access to information legislation is that it helps to support confidence in our democracy, which is not something that can be taken for granted in today's world. This independent oversight strengthens confidence on the part of the public that there is someone whose job it is to protect those rights while ensuring that the system and those who operate it have the necessary time to do their work. Many access requesters begin their journey because of some disagreement with the public body from whom they are seeking records. It is understandable, therefore, that there may be a lack of trust in that public body when it seeks to self-extend or negotiate an extension.

In those jurisdictions that have increased their statutory deadlines to respond to access requests, or that have given public bodies the right to self-extend, or that have given public bodies the authority to "negotiate" their own extensions with applicants, we have not seen any evidence that access to information coordinators have less work to do. Ultimately, all of the same work needs to be done. We simply propose that it continues to be done in such a way that does not undermine confidence in the access to information process, which we believe can be accomplished by maintaining current statutory deadlines and time extension processes.

Recommendation

Recommendation 2026-8: Maintain the current access to information timelines in section 16 and 23.

Overdemand by Applicants and Disregard

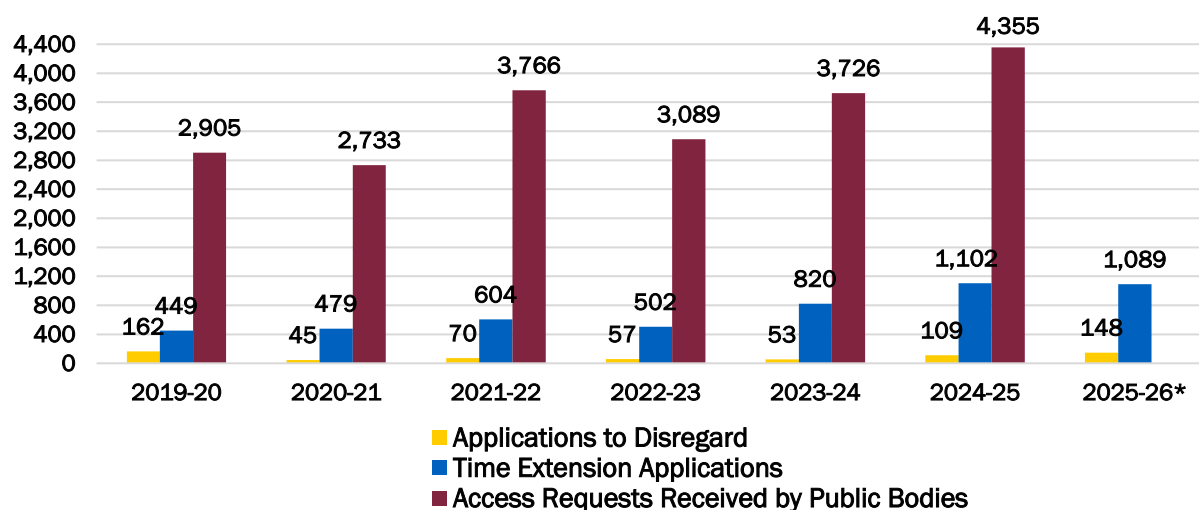
Currently, under ATIPPA, 2015, there are no limits on the number of access requests that an applicant can make, nor on how broad a request can be. There are examples of individuals making 10 plus requests in a single day to the same public body or requesting records that cover a whole topic for decades. There are individuals who, having become frustrated for their own reasons, whether consciously or not, have essentially weaponized the ATIPP process without regard to the impact on the public body's ability to carry out its mandate to serve the public, or even its ability to respond to other applicants. This has had a major impact on several smaller municipalities and has caused frustration for other public bodies as well. Over demand by a single applicant can strain resources and is not consistent with ATIPPA, 2015's purpose of strengthening accountability of public bodies to its citizens or having an open and transparent government.

It continues to be OIPC's position that there are remedies already available in ATIPPA, 2015 that adequately protect public bodies from frivolous and vexatious applicants, specifically, section 21 (Disregarding a request). A public body can apply to OIPC for approval to disregard a request. The grounds for approving a disregard are:

- the request would unreasonably interfere with the operations of the public body; OR
- the request is for information already provided to the applicant; OR
- the request would amount to an abuse of the right to make a request because it is:
 - trivial, frivolous, or vexatious or;
 - unduly repetitive or systematic or;
 - excessively broad or incomprehensible or;
 - otherwise made in bad faith.

The section on disregards granted by OIPC is quite broad and any one of the subsections on its own can justify the granting of a disregard by this Office. Section 21 gives public bodies the avenues they need to appropriately deal with overdemand by certain applicants. The section allows the head of a public body, within five business days of receiving an access request, to apply to the Commissioner for approval to disregard the request. Upon receipt of a disregard application the Commissioner has three business days to review and provide a decision to the public body.

Below is our statistical chart showing extension and disregard applications received by fiscal year. The chart shows that the increase in extensions and disregards correlates with the increase in number of access requests.



*2025-26 statistics for Access Requests Received by Public Bodies not yet published by the ATIPP Office.

One of the ongoing issues has been the short timeline that a public body has in order to apply for approval to disregard; that five-day period is often not enough time to determine whether a disregard is appropriate and then gather the evidence needed to complete the required form. The other circumstance we see is that public bodies have reached out to the applicant in an effort to clarify or focus the request, but there is not sufficient time within five business days to arrive at agreement. The public body, not knowing whether the applicant might agree to refine the request, is left with no choice but to apply for a disregard. Some of these disregard applications may not actually be necessary if the public body were given sufficient additional time to work with the applicant. On this point, OIPC agrees that increasing the number of

business days from five to ten that a public body has to apply for a disregard would be one measure to assist public bodies with this problem.

Another option for the Review Committee to consider is the authority that OIPC has to control its own processes, which may also work for public bodies if they have the same express authority in the Act. Section 44(7) states that:

44(7) Where the commissioner has 5 active complaints from the same applicant that deal with similar or related records, the commissioner may hold an additional complaint in abeyance and not commence an investigation until one of the 5 active complaints is resolved.

The section is limited in that the request must be from the same person, and the requests have to be for similar or related records. Our experience is that it helps us control our own processes and prevents us becoming overwhelmed by one complainant. It is our view that an abeyance section strikes a balance between ensuring individuals are not abusing the system and ensuring that access to information requests are carefully considered by the public body regardless of who is making the request. Creating an abeyance section for public bodies may also give them additional time to determine if a disregard application might be appropriate in the circumstances.

Recommendations

Recommendation 2026-9-1: Amend section 21(1) to increase the timeline for an application to the Commissioner for approval to disregard an access request from 5 to 10 business days.

Recommendation 2026-9-2: Amend ATIPPA, 2015 to provide authority for public bodies to hold in abeyance access requests over a certain number from the same applicant.

ACCESS TO INFORMATION PROVISIONS – ADMINISTRATIVE PROCEDURES

Terms of Reference Request: Review exceptions to access, timelines for response, and the effectiveness of current **administrative procedures** and the current cost schedule.

Informal Resolution Procedure

As noted in this Office's Annual Reports, OIPC works extensively with complainants, public bodies, custodians, and third parties to resolve complaints informally when possible and appropriate to do so. Historically, informal resolution has been the most common means of resolution for complaints made to this Office.

The current provisions of ATIPPA, 2015 that speak to the informal resolution procedure are found in the investigation section, specifically sections 44(3), (4), (5), and (6). The Act allows the Commissioner 30 business days from the date the complaint is received, to take appropriate steps to informally resolve a complaint. The 30-business day deadline can be extended for a further 20 business days by written request from both parties and the informal resolution process cannot extend past 50 business days. A final report from the Commissioner is due no later than 65 business days from the date the complaint is received.

There is currently a disconnect between the way the Act is written and the practical day-to-day investigation and resolution process followed by this Office. Most of the information gathering and investigatory analysis takes place during the first 30 business days, which is part of the informal period, but that time is spent opening the file, reviewing the complaint, gathering and reviewing records, and completing a preliminary investigatory analysis.

While the Act only requires the Commissioner to accept one submission from each party during the course of the entire investigation and that submission must be received by this Office within 10 business days of being notified of the complaint, in practice the Office may allow further submissions if necessary. The Office does not support extending the 10-business-day period for parties to provide their initial representations. In our experience, the current timeline functions effectively in the vast majority of cases and supports the timely

progression of investigations. Extending this period would delay the information-gathering process and could result in unnecessary delays in resolving complaints for all parties. Where needed, the Office already has the flexibility to consider additional submissions beyond the initial 10-business-day period.

It is our experience that the first 30 business days of the informal resolution period is spent on exchanging information and conducting analysis and that in almost all cases, the need to extend the informal resolution period is required. In practice, the extension of the informal resolution period is generally at the request of this Office and with the consent of the parties, rather than by written request of the parties as envisioned by the Act. While the Act also contemplates that the informal resolution period ends after 50 days, a complaint can be resolved by the parties up to the moment before a report is released, if for example a complainant belatedly decides they are satisfied and does not wish to continue with the process, or if a public body releases additional records, rendering the complaint moot. Finally, the Office has noted a chilling effect of “going formal”, making the parties less likely to continue working towards mutually beneficial resolution.

To better align the Act with practical experience, the Office recommends amending the Act to remove the requirement for parties to submit written requests for an extension of the informal resolution process and instead permit extensions at the discretion of the Commissioner. This recommendation is in keeping with the general principle that administrative bodies should control their own proceedings. The Supreme Court of Canada stated in [Knight v. Indian Head School Division No. 19, 1990 CanLII 138 \(SCC\), \[1990\] 1 SCR 653](#):

It must not be forgotten that every administrative body is the master of its own procedure and need not assume the trappings of a court. The object is not to import into administrative proceedings the rigidity of all the requirements of natural justice that must be observed by a court, but rather to allow administrative bodies to work out a system that is flexible, adapted to their needs and fair. As pointed out by de Smith (Judicial Review of Administrative Action (4th ed. 1980), at p. 240), the aim is not to create "procedural perfection" but to achieve a certain balance between the need for fairness, efficiency and predictability of outcome.

This Office will continue working diligently with both public bodies and complainants to ensure that as many matters as possible are resolved through informal resolution. A legislative amendment allowing the Commissioner to extend the informal resolution process at their discretion would assist the Office in achieving this goal.

Recommendation

Recommendation 2026-10: Amend the informal resolution extension provision to be at the discretion of the Commissioner.

Access to Information Complaints and Appeals

OIPC maintains its position as was set out at page 50 of our [Submission of the Information and Privacy Commissioner to the ATIPPA Statutory Review Committee 2020](#) and is reproduced in [Appendix C](#) for ease of reference.

Commissioner Vacancy

Although there is a provision for the appointment of an acting commissioner in ATIPPA, 2015, and provision for the commissioner to delegate their authority, there is no provision for the exercise of the commissioner's authority in instances of their incapacitation or if the office is vacated in the absence of such delegation or appointment. There have been several month-long vacancies after the retirement or resignation of a commissioner, and the failure to appoint an acting commissioner on a timely basis represents a serious reputational and legal risk to OIPC which could also impact complainants, third parties or public bodies.

Former Commissioner Ed Ring gave significant advance notice of his retirement, and he officially retired effective June 23, 2016. His replacement, Donovan Molloy, was not appointed until July 22, 2016. Former Commissioner Donovan Molloy resigned effective February 19, 2019, and an acting commissioner was not appointed until March 21, 2019. Former Commissioner Michael Harvey resigned effective May 5, 2024, and current Commissioner Kerry Hatfield was appointed December 5, 2024. There were alternating periods of an acting commissioner during this 6-month period, but the long vacancy caused difficulties.

ATIPPA, 2015 is written in such a way that every provision involving the exercise of the oversight role is one where the commissioner is empowered to do something. A compelling argument can be made that the oversight function can only legally operate where there is a commissioner in place. A delegation by a commissioner to staff arguably cannot survive when the commissioner's role is vacant.

It may have been assumed in regard to the appointment process that as long as a statutory deadline for a commissioner's report does not pass while the commissioner's role is vacant, then there are no concerns. This may not be correct.

For example, section 44 outlines the investigative process. Each aspect of the process involves the commissioner exercising authority under the statute, which is typically delegated to staff. This, or another challenging circumstance, could easily occur during a period of commissioner vacancy. While OIPC staff are knowledgeable in terms of carrying out the Office's oversight functions and are competent to take appropriate steps, without a commissioner, no one can be said to have been delegated to take those steps.

Furthermore, we have a number of ongoing court matters at any given time that require direction to counsel from the commissioner. Despite some awkward questions that have been put to us during these periods of time, staff have carried on with investigations, accepted new complaints, kept court proceedings moving and operated as if in a caretaker mode. Whether through luck or good faith on the part of the parties we deal with, staff have not yet been formally challenged on their authority to conduct oversight business, however this is not a solid foundation on which to operate.

In the absence of a commissioner, OIPC staff have been put in a very difficult position in attempting to continue to carry forward the Office's mandate without the confidence that the necessary authority exists to do so.

A challenge to our authority to operate without a commissioner is a serious reputational risk to the Office, regardless of outcome. Such a challenge could occur directly in relation to our oversight role, or in the legal arena where there are a number of matters to which we are a

party at any given time. In the legal arena, it is conceivable that a party could make an application for dismissal or removal of OIPC as an intervenor on the basis that OIPC counsel is without a client.

It is our position that there should not be a single business day without an acting commissioner in place upon the departure of a commissioner. Clearly, the administrative processes required to designate a commissioner, including an acting commissioner, require a certain amount of time under the current statutory provisions. Past practice is a reasonably good indication of future expectations, so in our view a legislative solution is required in order to avoid such circumstances.

One option to consider would be the designation of a specific position within OIPC who is authorized by statute to perform the duties of the commissioner in the case of the commissioner's incapacity, with no delegation of authority, or vacation of the office where an acting commissioner has not been appointed.

An alternative to that approach can be seen in Ontario's FIPPA, in which the Commissioner, at section 7.1(1), designates an individual employee of the Office "who shall have the powers and duties of the Commissioner if the Commissioner is absent or unable to fulfil the duties of his or her office or if the office becomes vacant." Unlike a delegation process which currently exists in section 103, this is a designation, which must be formalized and reported to the Speaker. Other than in narrow circumstances described in 7.2(2), the employee who has been designated in advance by the commissioner to carry out his or her function upon incapacitation, absence, or vacancy, would continue in that role until the appointment of a new commissioner for a full term, which ensures stability for the Office.

Recommendation

Recommendation 2026-11: Amend ATIPPA, 2015 to ensure that there is a designation of an office staff member to act in the role of Commissioner during any period where there is no acting commissioner or commissioner.

PRIVACY SAFEGUARDS AND EMERGING TECHNOLOGIES

Terms of Reference Request: Evaluate whether ATIPPA, 2015 adequately addresses risks associated with newly evolving technologies, including but not limited to: artificial intelligence; biometric data; and surveillance technologies.

Artificial Intelligence

Although we provided recommendations regarding artificial intelligence in our [2020 ATIPPA review submissions](#), as one can appreciate there have been further developments since then that warrant additional comments. With one exception that will be explained below, our submissions and recommendations from the 2020 review continue to represent our views. Our 2020 submissions on Artificial Intelligence (AI) are attached as [Appendix D](#).

AI is a massive, complex, and fast-evolving subject area that will be challenging to effectively assess and consider during this statutory review. That being said, there is also a corresponding urgency associated with AI because it is our belief that core government and other public bodies are already moving toward implementation of programs that involve the use of AI. One need only pay cursory attention to the news to gain some appreciation for the potential for massive benefit as well as the potential for massive harm that AI brings. Unfortunately, the harms are not always easily anticipated. They can arise in unexpected ways, and the means of identifying and preventing those harms are often unevenly implemented. The difficulty for us is that we are operating essentially in the dark, because there is no legal obligation on any public body to inform us or the public if they are using AI.

It's not necessary to include here any examples of AI applications that are working well, of which we can surmise there are many. It is also unnecessary to provide additional examples of AI gone wrong – of which there are also many. Our focus here is the lack of a statutory framework to protect the public when AI causes harm, either through a failure of due diligence, or through the inherent challenges of working with a technology that can be difficult to understand and predict.

To illustrate where we are at present with AI vis a vis public sector entities, we refer you to [Privacy Complaint Report PI21-0000, McMaster University](#), dated February 28, 2024, from the Ontario Information and Privacy Commissioner. Paragraphs 66 and 132 to 155 of that report illustrate the difficulties that arise when there is no legislation governing public sector use of AI. The Report outlines the challenges that the Ontario Privacy Commissioner faced in not having appropriate legislation to enforce guardrails for the use of AI in that province by entities that are otherwise subject to her oversight.

Despite acknowledging the absence of statutory provisions to ensure the safe use of AI by public bodies, and therefore the lack of any statutory authority for her to do so, Ontario's Commissioner proceeded to use her report to issue recommendations regarding the use of AI by public bodies. She did this, we believe, because privacy oversight is closely adjacent to the kinds of considerations that arise with the use of AI. While AI initiatives often involve the collection, use, and disclosure of personal information, the potential impacts and harms, as well as the preventative steps and mitigations, are outside the scope of most privacy statutes. In this case, the Commissioner apparently concluded that there was simply no other body or authority available who could make these recommendations, and in the public interest, felt obligated to bring them forward. I believe her recommendations were well-considered and appropriate. That being said, given that we know the kinds of harms and risks that can arise from the use of AI, it is simply not appropriate that oversight be left to privacy commissioners or any other body without a clear mandate and legal authority to carry it out.

OIPC is in a unique position as a regulator to play an oversight role as AI is integrated into our public service. With a broadened statutory mandate (as proposed in our previous ATIPPA submission) to consider not just privacy and access but other potential harms to society, OIPC can assist public bodies in ensuring that AI is used for the primary benefit of our citizens by promoting measures that can help assess and avoid harms.

A core element of any AI regulation must be a legislative requirement for all public bodies to complete algorithmic impact assessments for programs using AI that could impact humans. The specific threshold is something that could be defined in regulations. This will assist in

determining the risks, fairness and impacts of such systems, and is a basic due diligence process that is analogous to privacy impact assessment tools that are now standard practice.

Transparency and accountability will be necessary for the public to accept the use of AI and to prevent the plethora of harms that humans are becoming increasingly fearful of when discussing and using AI. This is why records must be maintained of any AI processing activities. Social license is the term that is often used to describe the degree of public consensus or support behind an initiative. Public and private sector entities are clearly moving forward with AI implementation at speed, while it is unclear whether the social license yet exists for the intensity of change we are witnessing. It is, however, clear to anyone who reads the news that people around the world are clamouring for effective and appropriate regulation and oversight of AI. Through regulation and independent, effective oversight, public trust, and consequent social license, may actually be generated. In some larger jurisdictions, this may mean a separate AI statute and a new oversight model. Until that occurs here, OIPC, as an existing oversight office which already has an adjacent mandate would appear to be a ready option. Any non-independent entity that purports to perform an oversight function while operating within government may not receive the same level of public trust or credibility.

Chair Orsborn agreed with our recommendations in his report following the 2020 statutory review of ATIPPA, 2015, however we wish to make one small adjustment to the recommendations in those submissions. Instead of notifying the Commissioner and requiring engagement on each use of AI, there should be a statutory mandate for government to publish a registry of AI impact assessments. The Commissioner should be entitled to require that a public body provide a particular AI impact assessment for review upon request, and the Commissioner should be enabled through clear statutory language to comment on any implications for the use of AI, such as those referenced by Ontario's Commissioner in her McMaster University report, or any other recommendations to mitigate any negative effects flowing from the use of AI, relating to or stemming from the collection, use, or disclosure of personal information, that could have impacts on individuals, groups, or the public at large.

Recommendations

Recommendation 2026-12-1: Incorporate a definition of artificial intelligence into ATIPPA, 2015.

Recommendation 2026-12-2: Require algorithmic assessments to be conducted by any public body prior to implementation of a program involving the use of artificial intelligence.

Recommendation 2026-12-3: Create a statutory requirement for a published registry of AI impact assessments, and a corresponding authority for the Commissioner to require that a public body provide a particular AI impact assessment for review upon request

Recommendation 2026-12-4: In addition to privacy and access to information issues, in its review and assessment, OIPC should be entitled to comment on all implications for the use of AI in the proposed program, including data ethics factors such as proportionality, fairness and equity, in a manner comparable to a Data Commissioner; to this end, amendments to the purpose of ATIPPA, 2015 would be required to reflect the added mandate for an independent oversight agency that is empowered to review and comment on the implications, including privacy and data ethics implications, for the implementation of artificial intelligence in public body programs. Comparable powers or duties would need to be added to section 95.

Recommendation 2026-12-5: Introduce a special Duty to Document requirement for artificial intelligence applications that requires that records of processing activities be maintained.

Biometric Data

Biometric information consists of data derived from an individual's unique physical or behavioural characteristics. Common examples include fingerprints, facial geometry, DNA, iris and retinal scans, voiceprints, gait patterns, handwriting characteristics, and typing patterns. Biometric technologies are increasingly used by governments and private-sector organizations for identification, authentication, security, and access-control purposes. Examples include fingerprint scanners, facial recognition systems that compare a live image to an enrolled facial

template, and voice recognition systems that analyze speech characteristics such as accent, rhythm, and pronunciation.

While biometric technologies can provide convenient and effective authentication, biometric identifiers are fundamentally different from passwords, account numbers, or access cards. Biometric characteristics are intrinsically linked to an individual and generally cannot be replaced or changed if compromised. A person can cancel a credit card or reset a password; however, it is impossible to change one's fingerprints, facial structure, or voice. As biometric technologies become more widespread and sophisticated, they present significant privacy risks. Threat actors can replicate fingerprints, use artificial intelligence to mimic voices, and exploit biometric information in ways that were not previously possible. Given the unique and permanent nature of biometric identifiers, their collection and use require careful oversight and robust privacy protections.

Although biometric technologies may offer security benefits, they also raise several significant privacy concerns.

1. **Function Creep:** Function creep occurs when information collected for one purpose is subsequently used for another purpose that was not originally identified or consented to. For example, an organization may collect an employee's facial metrics solely for building access control but later use that information to monitor employee attendance, movement, or productivity. Such secondary uses may exceed the original purpose for which the information was collected and undermine individual privacy expectations.
2. **Covert Collection:** Biometric information can be collected without an individual's knowledge or consent through surveillance technologies such as facial recognition systems, remote cameras, or voice analysis tools. Even where an individual initially consents to the collection of biometric information, there may be a loss of control over how that information is subsequently used, shared, retained, or disclosed.
3. **Surveillance and Chilling Effects:** The increasing use of biometric systems creates the potential for widespread monitoring and identification of individuals in public and private spaces. The possibility of being continuously identified or tracked may affect

individual behaviour and undermine privacy, anonymity, freedom of expression and freedom of assembly.

4. **Accuracy and Reliability Concerns:** Biometric systems are not infallible. Their accuracy may decline as individuals age, experience illness or injury, or undergo physical changes. Errors in biometric matching can result in false positives or false negatives, potentially affecting access to services, employment opportunities, or other important decisions.
5. **Security Risks:** Because biometric information is permanent, the consequences of a privacy breach can be particularly severe. Unlike passwords or account credentials, biometric characteristics cannot realistically be replaced once compromised. Organizations that collect biometric information therefore have an obligation to implement strong security safeguards to protect it from unauthorized access, use, disclosure, or theft.

Recognizing the growing use of biometric technologies, the Office of the Privacy Commissioner of Canada has published guidance documents for federal institutions processing biometric information, including:

- [Guidance on Processing Biometric Information for Federal Institutions](#); and
- [Biometrics: Quick Tips for Federal Institutions](#).

These documents emphasize the importance of necessity, proportionality, transparency, privacy impact assessments, and appropriate safeguards when deploying biometric technologies.

A significant example of the privacy risks associated with biometric technologies is the joint investigation conducted by the Privacy Commissioner of Canada and the privacy commissioners of Alberta, British Columbia, and Québec into Clearview AI Inc. The investigation found that Clearview AI had collected billions of facial images from publicly accessible websites and social media platforms without the knowledge or consent of the individuals concerned. The company used those images to create biometric identifiers and facial recognition databases that could be searched by users. The commissioners concluded

that Clearview's practices violated Canadian privacy laws. They found that Clearview collected personal information without consent by scraping individual's information from websites and conducted mass surveillance of Canadians, then used that data for inappropriate purposes.

The Clearview investigation illustrates the unique privacy concerns associated with biometric technologies and demonstrates the need for clear statutory safeguards governing their collection and use.

Legislation

The current definition of personal information in the Act at section 2(u) includes certain biological identifiers:

(v) the individual's fingerprints, blood type or inheritable characteristics.

While this provision recognizes some forms of biological information, it does not expressly address many modern forms of biometric information such as facial recognition templates, iris scans, voiceprints, gait analysis, or other emerging biometric technologies. As a result, the current legislative framework may not adequately reflect the sensitivity and breadth of biometric information now being collected and used.

Prince Edward Island

Prince Edward Island's [Freedom of Information and Protection of Privacy Act](#) expressly includes biometric information within the definition of personal information and provides a separate definition. The Act includes within personal information at section 1:

1. (a.2) "Biometric information" means information derived from an individual's unique measurable characteristics.
- 1.(i)(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics.

Alberta

Alberta's [Protection of Privacy Act](#) similarly recognizes biometric information as part of personal information and has its own definition:

- 1 (a) "biometric information" means information derived from an individual's measurable characteristics.

- (q) “personal information” means recorded information about an identifiable individual, including
- (v) the individual’s fingerprints, other biometric information, blood type, genetic information or inheritable characteristics.

Québec

Québec stands apart from other Canadian jurisdictions by establishing a distinct legislative framework governing biometric technologies. Under Québec's [Act to Establish a Legal Framework for Information Technology](#) and related privacy legislation, biometric information is treated as highly sensitive personal information. Organizations seeking to use biometric technologies must demonstrate that:

- the use of biometrics is objectively necessary;
- the proposed collection is proportional to the identified purpose;
- meaningful and express consent is obtained where required;
- less privacy-invasive alternatives have been considered; and
- the Commission d'accès à l'information (CAI) is notified before creating or deploying biometric databases.

Québec's framework provides a useful model for balancing innovation with strong privacy protections and public accountability.

Federal Developments

Recent federal legislative proposals have also recognized the heightened sensitivity of biometric information. The proposed Bill C-36 [Protecting Privacy and Consumer Data Act](#) (PPCDA) identifies biometric information capable of uniquely identifying an individual as a category of sensitive personal information. This reflects a growing recognition that biometric data warrants enhanced privacy protections due to its permanent, unique, and highly identifying nature.

Biometric technologies are not inherently incompatible with privacy. However, the collection, use, and disclosure of biometric information should be governed by clear legal requirements and strong accountability mechanisms. Any legislative framework governing biometrics should incorporate the following principles:

1. **Necessity and Legal Authority.** Organizations should collect biometric information only where they have clear legal authority to do so and where the information is demonstrably necessary for a legitimate purpose.
2. **Data Minimization** Only the minimum amount of biometric information necessary to achieve the authorized purpose should be collected.
3. **Purpose Limitation.** Biometric information should be used only for the purpose for which it was originally collected. Secondary uses should not be permitted unless specifically authorized by law or supported by appropriate consent.
4. **Transparency** Individuals should be informed about what biometric information is being collected, why it is being collected, how it will be used, who will have access to it, and how long it will be retained.
5. **Accuracy** Organizations should take reasonable steps to ensure biometric information remains accurate, complete, and up to date for the purpose for which it is used.
6. **Security Safeguards** Given the sensitive and permanent nature of biometric information, organizations should implement robust administrative, technical, and physical safeguards appropriate to the level of risk.
7. **Retention and Disposal** Biometric information should be retained only for as long as necessary to fulfill the identified purpose and should be securely destroyed when no longer required.
8. **Accountability and Governance** Organizations should establish clear governance structures for biometric systems, including policies, training, oversight mechanisms, and regular reviews of compliance.
9. **Privacy Impact Assessments** Privacy Impact Assessments (PIAs) should be required before implementing biometric systems to evaluate privacy risks, assess alternatives, and identify appropriate safeguards.

Biometric technologies offer significant opportunities to improve security, authentication, and service delivery. At the same time, they create unique privacy risks because biometric identifiers are highly sensitive, uniquely identifying, and generally cannot be changed once

compromised. For that reason, biometric technologies should be used extremely sparingly by public bodies, when no other practical options exist.

As biometric technologies become increasingly common, the legislative framework governing personal information should be modernized to explicitly recognize biometric information, establish clear rules for its collection and use, and ensure that appropriate oversight and safeguards are in place. By adopting a principled, risk-based approach, public bodies and private organizations can realize the benefits of biometric technologies while preserving the privacy rights of individuals and maintaining public confidence in their use.

Recommendations

Recommendation 2026-13-1: Amend section 2(u)(v) to expressly recognize biometric information within the definition of personal information:

- "(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics."

Recommendation 2026-13-2: Include a definition of "biometric information" as:

- "Information derived from an individual's unique measurable characteristics."
- This definition is consistent with the approaches adopted in Prince Edward Island and Alberta.

Recommendation 2026-13-3: That a Privacy Impact Assessment be mandatory for any program, initiative, or substantial modification involving the collection, use, or disclosure of biometric information.

Recommendation 2026-13-4: That public bodies be required to notify OIPC before implementing any program involving the creation of a biometric database and provide the completed Privacy Impact Assessment to the Office for review and comment before deployment.

Recommendation 2026-13-5: That legislation provides for independent oversight, investigations, complaint resolution, and enforcement mechanisms to ensure accountability and maintain public trust in the use of biometric technologies.

Surveillance Technologies

Privacy is a right that protects individual autonomy, prevents the misuse of personal data, and acts as a foundation for exercising democratic rights and freedoms. Without robust privacy safeguards, unchecked surveillance can lead to significant individual and societal harm.

When police and government respect privacy and inform the public why, when and how surveillance is being used, it builds the necessary trust that societies need to ensure public confidence. The opposite of this philosophy is the mass outcry in the United States about cameras operated by Flock Safety, a private technology company that provides automated license plate reader cameras and surveillance networks used by law enforcement and local communities. The Flock camera records license plate numbers, a vehicle's make and model and distinctive features such as color, bumper stickers and roof racks. The cameras log when and where a vehicle goes by, creating searchable travel histories for the vehicle. Flock operates hundreds of thousands of cameras in the U.S. and have become controversial because law enforcement can track vehicles in violation of a person's privacy without legal warrants. There have been cases where law enforcement personnel tracked an individual for their own personal reasons. Flock Safety is a private company and was found to have shared data to other municipal and federal jurisdictions which led to backlash against the company and calls to restrict the technology. While this is one of the worst-case scenarios, it is indicative of the unfortunate direction that private companies are taking towards privacy. Once the information is collected, it can also be misused by governments and law enforcement.

This Office has consistently outlined that any use of video surveillance by public bodies must comply with the Act and may only be collected pursuant to section 61 of the Act which states:

61. No personal information may be collected by or for a public body unless
 - (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.

In [Report P-2018-003](#) this Office investigated the Town of Paradise and its video surveillance of town properties including 69 cameras in public spaces and a further 18 cameras in staff only areas. This report outlined the legal requirements necessary for public bodies to comply with the Act and highlighted that there must be a “real, pressing and substantial” problem at the locations where the cameras were installed. The Town failed to provide the necessary evidence to justify the video cameras at Town buildings or in staff areas which resulted in the Commissioner’s recommendation that the Town cease the collection of personal information via the cameras.

Cameras are also increasingly prevalent in Canadian public spaces, which curtails our public anonymity and may deter people from exercising their constitutional rights such as freedom of speech or freedom of assembly. In 2025 this Office created a guidance piece entitled [“Use of Video Surveillance”](#) which provided public bodies with the necessary information to ensure compliance with ATIPPA, 2015 and PHIA. The use of video surveillance can be highly intrusive to privacy, and all protections must be put in place prior to any program being implemented. We refer to [Report P-2021-002](#) where the Town of Happy Valley-Goose Bay initiated a program for a municipal enforcement officer to wear body worn cameras. The Commissioner recommended the cessation of the program until the Town could demonstrate full compliance with the Act, develop a privacy management program, complete a privacy impact assessment and update its policies accordingly. This report outlines what can happen when the Act is not fully considered before implementing a surveillance program.

Recommendations

Recommendation 2026-14-1: Require all organizations to conduct a privacy impact assessment prior to using video surveillance.

Recommendation 2026-14-2: Require all organizations who use video surveillance to have a privacy management program and policies in place that ensure compliance with the Act.

PERSONAL INFORMATION PROTECTION

Privacy and Political Parties

The Information and Privacy Commissioner under ATIPPA, 2015 is responsible for, among other things, being an advocate for privacy (section 3(1)(f)(i)). We take this mandate seriously in many different facets, ranging from our recent youth privacy video series [Think Digital Privacy](#), to the white paper we published in 2020 (updated in 2026), entitled [Internet Voting – Privacy and Security Risks](#). Advocacy, by its nature, extends beyond compliance with existing laws. It must also occur when new privacy issues arise, whether as a result of the availability of new technologies, because of changing societal expectations, or because there have been proposals for new laws or policies. Being able to advocate for the privacy of Newfoundlanders and Labradorians, in any context that affects them, is a core part of the Commissioner’s role.

On April 30, 2026, Alberta’s Information and Privacy Commissioner issued a [statement](#) of deep concern that a group affiliated with a provincially-registered Alberta political party had created a publicly accessible database containing the names, addresses, and in some cases phone numbers, of almost three million Alberta voters. The source of the information was the List of Electors maintained by the Chief Electoral Officer of Alberta, to which registered political parties are entitled to have access.

In a [release](#) dated May 1, 2026, Alberta’s Chief Electoral Officer stated, “As the legislation is currently written, Elections Alberta cannot prevent an unauthorized distribution or use of a List of Electors provided to a registered political party or other authorized entity.” Further, the Chief Electoral Officer’s statement reads: “Elections Alberta supports the Information and Privacy Commissioner of Alberta’s April 30th statement regarding the need for legislation that protects the personal information of Albertans that is in the hands of registered political parties.”

The statement from Alberta’s Information and Privacy Commissioner that was supported by Alberta’s Chief Electoral Officer reads as follows:

The List of Electors is obtained under the Election Act from the Chief Electoral Officer as is authorized by that Act. This Act (section 18) requires the Chief Electoral Officer to distribute a List of Electors to political parties, non-party-affiliated members of the Alberta Legislative Assembly, and to potential candidates in certain circumstances and for specified purposes. The Election Act governs use and disclosure of this information by those who are permitted to receive it. While the Election Act has some controls concerning the List of Electors, this law does not protect the privacy rights of Albertans concerning their personal information and does not have the strong privacy protections that are in PIPA to protect these rights.

“This is evidence of a concerning gap in Alberta’s privacy laws as it relates to the collection, use and disclosure of personal information by political parties,” concluded McLeod. “This gap has been recognized by my office, which has been calling for PIPA to be amended to include political parties for decades. During the PIPA review, which is still underway, we renewed the call for political parties to be made subject to the Act. Of note is that BC’s PIPA, which is substantially similar to Alberta’s, does apply to BC’s political parties. I am once again calling on government to make political parties subject to PIPA in the next set of amendments to the Act.”

This breach of Alberta’s List of Electors has spawned multiple investigations. The RCMP is investigating to determine whether there was any criminal activity implicated in the breach. The Chief Electoral Officer is investigating to determine whether Alberta’s elections law was violated. Alberta’s Privacy Commissioner is investigating the third party, which is a private company, to see whether it may have violated Alberta’s private sector privacy law. Class action lawsuits have also been filed in this matter. The bottom line, however, is that this breach happened, and there were very few statutory safeguards in place to prevent it from occurring. Furthermore, the number of investigations and legal proceedings is indicative of the fact that there is not only an absence of law, there is an absence of clear oversight specifically relating to privacy and security matters for information held by political parties.

The context is much broader than the events in Alberta. Today, political parties can collect and use data about citizens in order to target very specific voters for very specific messaging. They can engage social media platforms and other advanced data analytics tools to target messaging. Such tools were already available prior to the advent of artificial intelligence, which has only served to supercharge their potential impact.

The continuum between campaigning for votes and engaging in voter manipulation may not be as broad as we might hope. Data collected and used by political parties could also be provided to third parties which engage in outright misinformation. There are numerous companies out there already that offer some version of these tools. The question is, can it occur, and if a political party were tempted to pursue some of these activities, do any laws apply that would restrain such practices? These are rhetorical questions, because it is difficult to refute the conclusion that political parties are among the least regulated entities in Canada, but hold some of our most personal information.

There is an exception, however. British Columbia's private sector privacy statute, the Personal Information Protection Act (PIPA), currently applies to provincial political parties in that province. The BC Supreme Court had issued a ruling which found that it also applied to federal political parties, however the federal government quickly passed a law specifying that provincial laws do not apply to federal political parties. That federal law, called the *Strong and Free Elections Act*, contains requirements that political parties develop privacy policies, but there are numerous gaps, as [outlined](#) by Professor Michael Giest. The law has weak enforcement provisions and lacks a number of standard elements of any privacy law. It is therefore not a model to be emulated in Newfoundland and Labrador.

In British Columbia the applicable privacy statute is a broad private sector privacy law which happens to also capture political parties. We do not have such a law in this province, however we can get to the same place without going the same route as BC did. There is no reason why Newfoundland and Labrador, or indeed any other province, could not develop a narrowly-focused set of provisions that specifically apply to provincially-registered political parties, without needing to pass a broad privacy law that would apply to all private sector entities. Such provisions could be designed to address the ten privacy principles upon which most modern privacy statutes are based, to ensure that they will fill the gap that Alberta's unfortunate events have highlighted, and also ensure that they measure up to the standard of private sector privacy laws such as the one in British Columbia. Such provisions dealing with privacy and political parties could be included within ATIPPA, 2015, as we are proposing, or if government chooses, it could also be a standalone statute. Either way, it is clearer than ever that such a measure is well warranted.

At [page 182](#) of the Report of the 2014 Review of ATIPPA, chaired by former Premier and Chief Justice Clyde Wells, there is an analysis of the issues relating to privacy and political parties, and a clear recognition that the lack of any legislation protecting the privacy of Newfoundlanders and Labradorians was “a gap” and “an area of concern.” While the 2014 ATIPPA Review Committee did not consider this topic to be part of its formal mandate, it did take the time to outline what those concerns were in order to draw these problems to the attention of government.

The review of ATIPPA, 2015 that was led by former Chief Justice Orsborn took the opportunity to consider this issue more deeply, perhaps recognizing that it was becoming more pressing over time as technological advances exponentially increase the potential invasiveness of the ways that personal information can be collected or used. Furthermore, the comments we made at page 39 of our [written submission](#) continue to be relevant, and our comments here augment those.

Chair Orsborn agreed with our representations that political parties were in need of statutory regulation in order to protect the privacy of Newfoundlanders and Labradorians. He felt, however, that the issue was more complex than he was able to address in the context of all of the other issues raised in his review of ATIPPA, 2015, so he declined to sketch out a specific legislative approach. He did, however, make a clear [recommendation](#):

That government proceed expeditiously with the development of a regulatory and oversight regime covering the collection, use and disclosure of personal information by registered political parties.

The government of the day did not move expeditiously to develop the regulatory and oversight regime recommended by Chair Orsborn, and to date, government has not announced any plans to take the steps outlined in that recommendation. We now echo that recommendation, and we repeat our previous submissions on this subject, but we do add one important element of emphasis that was perhaps not as obvious during the previous reviews of ATIPPA. Based on the experience in Alberta, it is essential that any law governing the collection, use, and disclosure of personal information by political parties must have clear enforcement and

oversight provisions in order for it to be effective in protecting the privacy rights of Newfoundlanders and Labradorians.

Recommendation

Recommendation 2026-15: That government implement statutory privacy protections and independent oversight for personal information held by political parties.

Enhanced Safeguards for Sensitive Categories of Data

Terms of Reference Request: Consider the need for enhanced safeguards for sensitive categories of data;

ATIPPA, 2015, like most public sector privacy statutes, is written to be technology neutral. In other words, it operates at a high level and typically does not contain prescriptive provisions. For that reason, it is difficult to know, without further detail, what this section of the terms of reference is intended to pursue.

Some version of section 64 is fairly common in public sector privacy statutes, in that it establishes a requirement that public bodies “take steps that are reasonable in the circumstances” to protect person information against breaches and other harms outlined in that section. The phrase “reasonable in the circumstances” is understood to essentially require public bodies to protect personal information through measures commensurate with the sensitivity of the data. So, to that extent, ATIPPA, 2015 already contains a requirement to protect any and all personal information to the degree appropriate to the sensitivity of that information. This is an interpretation that we have relied in on in a number of past reports, including our [report into the cyber attack on the province’s health care system](#), which included both personal health information subject to the Personal Health Information Act, as well as personal information of regional health authority employees, which is subject to ATIPPA, 2015. One can find similar approaches in reports by Commissioners across Canada.

Recommendation

Recommendation 2026-16: Should government wish to introduce more prescriptive protections for specific categories of data, we would like to be consulted on the specific proposed language for such protections.

Rights of a Minor

Terms of Reference Request: Consider whether clarification is required around the rights of a minor in accessing or protecting their personal information.

To our knowledge, the rights of minors has not arisen as a significant issue in relation to ATIPPA, 2015. It has come up in the past several months in relation to the **Personal Health Information Act** (PHIA), and we have provided a [submission](#) on it in the context of the review of that Act, which is ongoing at the time of our preparation of this submission, and we refer you to that submission for some insight as to our views.

Recommendation

No Recommendation.

Indigenous Issues

OIPC maintains its position as was set out at page 47 of our [Submission of the Information and Privacy Commissioner to the ATIPPA Statutory Review Committee 2020](#) and is reproduced in [Appendix E](#) for ease of reference.

PRIVACY BREACH MANAGEMENT

Privacy Breach Notification Requirements and Timelines

Terms of Reference Request: Review the effectiveness of current privacy breach notification requirements and timelines;

Notification Requirements

ATIPPA, 2015 establishes notification requirements for both individuals impacted by a breach and OIPC. This requirement was new with ATIPPA, 2015. [Section 64 of ATIPPA, 2015](#) states, in part:

- 64 (3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is
- (a) stolen;
 - (b) lost;
 - (c) disposed of, except as permitted by law; or
 - (d) disclosed to or accessed by an unauthorized person.
- (4) Where the head of a public body reasonably believes that there has been a breach involving the unauthorized collection, use or disclosure of personal information, the head shall inform the commissioner of the breach.

This section of our submission will focus on the notification requirements to individuals while the following section, which examines public body reporting, will focus on the notification requirements to OIPC under section 64(4) of ATIPPA, 2015. As noted above, section 64(3) requires the public body to notify impacted individuals at the first reasonable opportunity, where personal information is either stolen, lost, disposed of except as permitted by law or disclosed to or accessed by an unauthorized person.

OIPC has issued a number of reports that assess notification requirements. The notification requirement does not just inform impacted individuals of the breach, it also helps impacted individuals determine steps to take to protect themselves from further harm.

Report [P-2008-001](#) describes the process of evaluating risks, stating:

Further considerations in evaluating the risk include determining the cause and extent of the breach, which can indicate whether the information was lost or stolen, or whether the breach was deliberate or accidental, whether the information can be recovered, or whether the breach was due to a systemic problem or an isolated incident. The process of evaluating the risk also includes identifying who and how many people may have been affected by the breach, as well as assessing the foreseeable harm which might come from the breach.

Report [P-2008-003](#) flagged how evaluation of the risks to impacted individuals feeds into the notification process, stating:

This analysis assists in determining whether notification is necessary, and if so, how it should be done and what information it should contain. The more sensitive the information, the more important the notification and the manner in which it is done becomes. Once people are aware of the breach and what information was potentially or actually exposed, they, along with the public body, can take appropriate steps to mitigate any potential risks associated with the information being disclosed.

OIPC's recent report [P-2023-001/PH-2023-002](#) also examines notification, explaining that "Reasonable notification requires that enough information be provided to allow the individual to understand the significance of the privacy breach, and should include information that might assist the individual in reducing or preventing harm that could be caused by the privacy breach." It further states, "Mitigation of harm impacts decisions about whether to notify, who to notify, how to notify, and what information to include in the notification."

While the Act states that notification must occur at the first reasonable opportunity, it does not specify "how" notification should occur. This means that the method of notification must be assessed based on the particular circumstances of the privacy breach. Notification in report [P-2023-001/PH-2023-002](#) involved a mixture of direct and indirect notification. Direct notification is when an individual is notified of the privacy breach in person, by telephone, mail, email, virtual meeting, or other such forms of communication. Indirect notification is when an individual is notified of the privacy breach by a form of public communication. Indirect notification can include public announcements such as public advisory briefings, news releases, website notifications, social media postings, newspaper advertisements, and other

such similar measures. The report identifies critical content for notifications, which is similar to the requirements found in Alberta's [Protection of Privacy \(Ministerial\) Regulation](#).

Report [P-2023-001/PH-2023-002](#) outlined what information should be included in notifications. Paragraph 151, in part, stated:

...

Notifications should include the following information:

- Date of the breach (if the date is not known, the period during which the breach occurred, and if that is unknown, the approximate period);
- General description of the circumstances of the breach;
- Description of the information;
- Steps taken so far to control or reduce the harm;
- Future steps planned to prevent further privacy breaches;
- Steps the individual can take (a description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm);
- Organization contact information that the affected individual can use to obtain further information about the breach;
- Our Office's contact information and notification of an individual's right to make a complaint.

The report concluded that there was a delay in communicating critical factors to impacted individuals, namely that it was a ransomware attack.

Report [P-2026-001](#) also examined notification, stating,

Immediately after becoming aware of the incident, the Department moved to ensure that known information was communicated to the public, issuing public advisories, providing information online, disseminating information to schools, to our Office, and the Newfoundland and Labrador Teachers' Association, reflecting an early recognition of the need to manage potential harms.

Regarding this breach, the one aspect of notification that was flagged as unreasonable was the failure to use direct notification for students where a number, described as a “potential social insurance number” was impacted in the breach.

A number of Canadian jurisdictions require notification based on the “real risk of significant harm.” Section 10.1(1) of the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) requires notification to the commissioner and section 10.1(3) requires notification to impacted individuals if the breach creates a real risk of significant harm. The notification should be completed “as soon as feasible”. Sections 10.1(7) and (8) define significant harm and the factors to consider in determining the risk of a breach, stating:

- (7) For the purpose of this section, *significant harm* includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.
- (8) The factors that are relevant to determining whether a breach of security safeguards creates a real risk of significant harm to the individual include
 - (a) the sensitivity of the personal information involved in the breach;
 - (b) the probability that the personal information has been, is being or will be misused; and
 - (c) any other prescribed factor.

ATIPPA, 2015 also has a “significant harm” requirement included in subsections 64(7), (8) and (9) as follows:

- (7) Subsection (3) does not apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information.
- (8) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.
- (9) The factors that are relevant to determining under subsection (7) whether a breach creates a risk of significant harm to an individual include
 - (a) the sensitivity of the personal information; and
 - (b) the probability that the personal information has been, is being, or will be misused.

The head of the public body does not need to notify an individual of a breach if they reasonably believe that the breach does not create a risk of significant harm to the individual who is the subject of the information. The Act outlines what is considered “significant harm”, such as, bodily harm, humiliation, damage to reputation or loss of employment, financial loss, identity theft etc. and the factors relevant for determining whether a breach creates a risk of significant harm include the sensitivity of the personal information and the probability that the personal information is or will be misused.

An individual’s personal information may be the subject of a privacy breach and yet that individual would not be notified based on a public body’s assessment of the breach and the “risk of significant harm”. However, subsection 64(5) of ATIPPA, 2015 states:

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

The Commissioner can still recommend that the public body notify an individual of a privacy breach.

A number of provincial laws also require mandatory notification of affected individuals, for example:

- Section 36.3 of BC’s [Freedom of Information and Protection of Privacy Act](#) (FIPPA) addresses breaches. They define a privacy breach as, “the theft or loss, or the collection, use or disclosure that is not authorized by this Part, of personal information in the custody or under the control of a public body.” The legislation also relies on notification “without unreasonable delay” when there is a significant risk of harm to the impacted individual.
- Section 10(2) of Alberta’s [Protection of Privacy Act](#) (POPA) requires notification to the impacted individual, the Commissioner and the Minister without unreasonable delay if the breach raises real risks of significant harm. Section 4 of the [Protection of Privacy \(Ministerial\) Regulation](#) establishes considerations when assessing real risk of

significant harm, as well as mandatory content for notifications to impacted individuals, the Commissioner and the Minister.

Recommendations

Recommendation 2026-17-1: Prescribe in the regulations the content that should be included when notifying affected individuals of a breach.

Recommendation 2026-17-2: Require breaches to be reported to the Minister responsible for ATIPPA, 2015 (as required by Alberta's POPA) and other interested parties (as required under PIPEDA). The breach reports should be done at the first reasonable opportunity.

Timelines

Section 64(3) of ATIPPA, 2015, does not provide a specific timeline for notification to an individual, only requiring the public body to notify impacted individuals at “the first reasonable opportunity”.

Privacy breaches can be significant, large, and impactful but they could also be small and involve an isolated incident that is easily contained. Every privacy breach is unique with different considerations, and the timing of the notification will also depend on various factors.

OIPC's recent report [P-2023-001/PH-2023-002](#) examines timing of notifications, noting,

What that “first reasonable opportunity” is, might not be the same in every case, and will depend on the particular circumstances of the privacy breach. While it could be the same day in some instances, or several days in others, public bodies and custodians are accountable for their notification decisions, including their interpretation of when they deemed “the first reasonable opportunity” to be.

Recommendation

No Recommendations.

Public Body Breach Prevention, Response, and Reporting

Terms of Reference Request: Assess the adequacy of public body obligations for breach prevention, response, and reporting.

While OIPC has not conducted a systemic audit of breach reports received by our Office or surveyed public bodies, we have noticed trends over the past decade, which are reflected below.

Breach Prevention

It is not possible to eliminate privacy breaches altogether; however good prevention strategies can help keep occurrences to a minimum.

When a breach occurs, it is essential for a public body to conduct an investigation into the breach to fully understand what happened and identify root causes and to evaluate factors that contributed to the breach. This is one of the key steps in mitigating the risk of a future breach. The end result should be that the risks identified during the investigation are addressed to the fullest extent possible.

Privacy breach prevention can also include implementing, reviewing, and updating policies that deal with protection of personal information, training staff on privacy best practices and ensuring privacy safeguards are in place.

In reviewing breach reports, OIPC has noticed that public bodies sometimes identify prevention activities that may not assist in preventing future breaches. In some reports public bodies indicate that an employee involved in a breach will repeat the ATIPP Online Training and while this may be somewhat helpful, that training is not designed to prevent breaches as it is only a general training program. A more effective preventative measure might be a manager or privacy officer having a discussion with an employee who was involved in a breach. For example, if an individual has misdirected an email, their manager or the privacy officer may discuss with them the best practices when sending emails and explain the impact a misdirected email may have on an individual.

Breach Response

The Access to Information and Protection of Privacy (ATIPP) Office created a “Privacy Breach Protocol” to assist public bodies with making decisions when a privacy breach occurs. In our view, this protocol is a useful framework for responding to a privacy breach. The Privacy Breach Protocol (March 2015) identifies four key steps of managing a privacy breach:

1. Contain the Breach;
2. Evaluate the Risks;
3. Notify Affected Individuals (if appropriate);
4. Prevent Future Breaches.

The Privacy Breach Protocol is only useful if public bodies and employees know it exists. When a public body becomes aware that there has been a privacy breach, staff should know how to respond. What steps must be taken, who has to be contacted, what containment and mitigation measures need to be implemented, who has been affected, what notifications need to be provided and what prevention measure should be put in place. For all staff to have this knowledge, they must have training on privacy breach protocols and the public body should have policies and procedures in place so that if a breach is identified then staff can follow those policies and procedures.

OIPC has received many calls over the years after notification letters have been distributed to individuals from public bodies. Some of these callers want to file complaints, however many times the impacted individual has not been able to reach anyone at the public body and is calling OIPC for more information about the breach. When a public body is sending notifications to impacted individuals, it needs to ensure that it has the resources required to respond. OIPC has seen public bodies hire call centres for large breaches, however such investments are usually not necessary. A straightforward but effective step would be to publish a dedicated phone number that is consistently answered and to ensure sufficient staff are available to support the primary contact. Together, these measures would significantly improve a public body’s response to a privacy breach.

Overall, public bodies require adequate resources to be able to prevent, mitigate, and respond to breaches. In the absence of appropriate resources, public bodies cannot assess and critically analyze privacy breaches. Rather than being able to understand the root cause of the breach and the contributing factors, they are left with a cursory review. Public bodies simply do not have the time or the people to examine larger environmental factors that may contribute to a breach.

Recommendation

Recommendation 2026-18-1 (for Breach Prevention and Breach Response): Public bodies should have specific policies and procedures in place outlining what a privacy breach is and how to deal with it.

Breach Reporting

As noted above, ATIPPA, 2015 establishes requirements for notification of individuals impacted by a breach and reporting to OIPC. Notification to individuals under section 64(3) of ATIPPA, 2015 was discussed in the previous section and reporting to OIPC is contained in section 64(4) as follows:

64(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.

It is interesting to note that PIPEDA addresses notification to other interested parties in section 10.2(1), such as other organizations, a government institution or a part of a government institution, when the other entity may be able to reduce the risk of harm. PIPEDA's [Breach of Security Safeguards Regulations](#) establishes expectations for reporting the breach, the need to keep the Commissioner's Office up-to-date on new developments, sending details using a secure means of communications, the content of notifications for impacted individuals, the means of notifications, and recordkeeping.

OIPC has created a number of resources to assist public bodies, including a [form](#) for reporting privacy breaches, as well as detailed [instructions](#) on how to complete the form. OIPC's guidance states, in part, "OIPC encourages and appreciates when a public body informally advises that a privacy breach has occurred and formal notification is pending, however this

informal step is not notification within the meaning of section 64(4) of ATIPPA, 2015.” OIPC appreciates that some public bodies may be uncertain about when to file a breach report, particularly when some details are still emerging, however, the breach report still must be filed to fulfill the reporting requirement to the commissioner.

Section 64(4) of ATIPPA, 2015 operates as a mandatory reporting of privacy breaches to the commissioner. OIPC has now had over 10 years of experience with this section of ATIPPA, 2015 and believes that it works well. In contrast, the [Personal Health Information Act](#) (PHIA) requires that only material breaches be reported to OIPC and it has been our experience that many custodians spend as much time assessing if the breach should be reported to OIPC as they do on other aspects of breach management.

Reporting a breach to OIPC provides us with an opportunity to ensure that the public body has included sufficient information describing the breach, ensure that the affected individual has been or will be notified if necessary, and review what action the public body has taken to contain the breach, mitigate the impact (if possible), and prevent future such breaches.

Notification of the affected individual is extremely important, especially if that person needs to assess any potential harm coming from the breach. Should the public body decide not to notify an individual and not provide an explanation in the breach form for not notifying, OIPC can follow up to ascertain whether notification is necessary or not.

Subsection 64(5) of ATIPPA, 2015 allows the Commissioner to recommend that the public body notify an individual even if was determined that notification was not required. Subsection 64(5) states:

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

This is extremely important, and in our view, could be strengthened to allow the Commissioner to “require” the public body notify the individual. This is also why mandatory reporting of

privacy breaches to this Office is important so that the notification requirements and risks can be reviewed.

OIPC may also decide to follow-up with questions, clarifications, or suggestions regarding containment or prevention measures. Should a report not contain enough information to assess the breach, OIPC has the ability to request the public body to take further steps and update the breach report. Even when OIPC does not follow-up on a breach report, the requirement to report breaches and meet established reporting standards serves as an important quality control mechanism for public bodies. To date, breach reports appear to have been filed in good faith.

OIPC publishes the number of breach reports received at our Office in our annual report, as well as in our quarterly ATIPPA newsletter, [Above Board](#). Email and mail issues are the most common types of breaches reported to our Office. Being able to track the types and frequency of breach allows OIPC to target our guidance and education regarding privacy breaches.

Year	ATIPPA Breach Notifications Received by OIPC
2015-2016	213
2016-2017	183
2017-2018	201
2018-2019	240
2019-2020	214
2020-2021	215
2021-2022	207
2022-2023	190
2023-2024	185
2024-2025	162
2025-2026	185
Total	2,195

Section 64(4) of ATIPPA, 2015, does not provide a specific timeline for notification, to OIPC only requiring the head of the public body to “inform” the Commissioner of the breach. OIPC has observed variations in reporting of breaches. Some public bodies will wait to report a

breach until they have all the necessary information while other public bodies will report breaches in chunks over time. While the latter is preferable to the former, both these practices delay reporting to OIPC and could be improved upon.

Containment and notification measures can be critical during the initial stages of a privacy breach response, as they can have the greatest impact on managing the incident. This is why it is important to report breaches to OIPC in a reasonable timeframe with whatever details are available. OIPC can then determine if any follow-up is needed, suggest containment measures, and provide general information in response to inquiries if necessary. In an effort to have public bodies report breaches in a timely manner, an amendment to section 64(4) requiring the breach report to be reported to the commissioner at the first reasonable opportunity would assist with this issue.

Recommendations

Recommendation 2026-18-2: Continued mandatory reporting of all breaches to OIPC.

Recommendation 2026-18-3: Amend section 64(4) of ATIPPA, 2015 to include reporting the privacy breach to the commissioner “at the first reasonable opportunity”.

Recommendation 2026-18-4: Amend section 64(5) of ATIPPA, 2015 to allow the commissioner to “require” the head of the public body notify the individual.

PUBLIC BODY PRACTICES AND ACCOUNTABILITY

Terms of Reference Request: Evaluate the privacy management frameworks of public bodies, including the role of Privacy Impact Assessments and mandatory training;

Privacy Management Frameworks

The following is general commentary on privacy management frameworks, with specific focus on privacy impact assessments and training. In order for OIPC to evaluate the privacy management framework of public bodies, OIPC would need to examine the framework in place

in each public body in detail. With the time available to prepare the submission, it was not possible to complete this work. The following reflects research as well as OIPC's experience investigating and guiding public bodies.

While ATIPPA, 2015 does not explicitly require public bodies to have a privacy management program, OIPC strongly believes that it is an important program that all public bodies should have. A privacy management program ensures that organizations build in privacy to all initiatives, programs, or services, and assists in meeting legislative privacy obligations. OIPC has created and published resources on its [website](#), including a step-by-step guidance piece on how to implement such a program titled "[Privacy Management Program](#)" along with an additional tool "Privacy Management Program – Gap Analysis", to assist with program development. OIPC has recommended these guidance pieces to all public bodies.

When initially developing guidance on privacy management frameworks, OIPC researched frameworks generally, as well as what resources and methods other jurisdictions used. Joint guidance produced by the Office of the Privacy Commissioner of Canada and OIPC British Columbia and Alberta, [Getting Accountability Right with a Privacy Management Program](#), stood out as an excellent resource which our office leveraged. OIPC adopted a privacy management program approach that centered on accountability; public bodies are responsible for protecting personal information in their custody or under their control and must be able to demonstrate this.

All public bodies are subject to Part III of ATIPPA, 2015 (Protection of Personal Information). This Part establishes authorities for public bodies to collect, use and disclose personal information. It also establishes that they must collect, use and disclose the minimum amount of personal information for the identified purpose and that information must be protected with reasonable safeguards. To comply with ATIPPA, 2015, public bodies must know what information they have, where it is stored, how it moves and how long it is retained. This is where privacy management program controls work together to form a foundation of compliance. OIPC's "Privacy Management Program" guidance identifies the following program controls:

- Inventory of personal information;
- Policies;
- Training;
- Breach management response procedures;
- Privacy and security risk assessment tools;
- Information sharing agreements;
- Transparent communication with individuals.

Some cross-jurisdictional examples provide further perspective. Section 36.2 of BC’s [Freedom of Information and Protection of Privacy Act](#) states, “The head of a public body must develop a privacy management program for the public body and must do so in accordance with the directions of the minister responsible for this Act.”

Section 25 of Alberta’s [Protection of Privacy Act](#) requires public bodies to establish and implement a privacy management program that complies with the prescribed regulations. The [Protection of Privacy \(Ministerial\) Regulation](#) details what privacy management programs must include and addresses additional information that must be included if the public body has custody or control of a high volume of personal information or highly sensitive personal information. The regulations also require public bodies to have a process for making their privacy management program available to the public upon request or publish it on their website.

Recommendation

Recommendation 2026-19: Require all public bodies to establish, implement, and maintain comprehensive Privacy Management Programs. If critical content is identified in regulations, it should differentiate between public bodies with different capacities, such as smaller municipalities, from larger public bodies with high volumes of sensitive personal information, such as the Department of Government Services.

Privacy Impact Assessments

Privacy Impact Assessments (PIAs) are tools that identify and evaluate the potential effects that a project, initiative, or proposed system or scheme may have on privacy. They identify

risks and recommend mitigation activities that could be undertaken to reduce identified risks as much as possible. Even when not required by law, it is best practice to conduct such an assessment, as public bodies must be in compliance with ATIPPA, 2015, with or without a PIA. When an organization is unsure if a PIA is required, they can conduct a preliminary PIA, or PPIA. This is a tool that examines the initiative at a high level to determine if a full PIA is warranted. If it is determined that a full PIA is not required, the reasons for this conclusion should be documented as part of due diligence and accountability.

The term "Privacy Impact Assessment" is defined in section 2(3) of ATIPPA, 2015:

- (w) "privacy impact assessment" means an assessment that is conducted by a public body as defined under subparagraph (x)(i) to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act;
- (x) "public body" means
 - (i) a department created under the Executive Council Act, or a branch of the executive government of the province,

Although all public bodies are subject to the requirements of Part III of the Act, the requirement for a PIA only applies to departments and branches of the executive government. This gap should be addressed. All public bodies should be assessing initiatives to ensure appropriate privacy protections are in place. Further, many entities currently not required to conduct PIAs by law are handling large volumes of personal information. At a minimum, new statutory language should encompass large entities that are not captured by the current definition, such as the Royal Newfoundland Constabulary and the City of St. John's. Both examples are already conducting PIAs, as they have both shared courtesy copies of previous PIAs with OIPC, so expanding the requirements should not create undue hardship.

While the requirement to conduct a PIA varies in legislation across Canada, all entities subject to privacy legislation must protect the personal information in their custody or under their control. Some examples of PIA requirements in legislation include:

- British Columbia's [Freedom of Information and Protection of Privacy Act](#). Section 69(5) requires the head of a ministry to conduct a PIA in accordance with the directions of

the minister responsible for this Act. Section 69(5.3) extends this requirement to the heads of all public bodies.

- Alberta's [Protection of Privacy Act](#). Section 26(1) requires public bodies to complete PIAs in prescribed circumstances; regulations determine if PIAs need to be submitted to the Commissioner's Office. Section 26(2) identifies critical content for PIAs and 26(3) establishes that public bodies must provide a copy of a PIA to the Commissioner within 30 business days of a request made under section 27(1)(j).
- Ontario's [Freedom of Information and Protection of Privacy Act](#). Section 38(3) requires the head of an institution to ensure a written assessment is prepared prior to collecting personal information; the section also establishes critical content for the assessment. Similar provisions (section 28(3)) in the [Municipal Freedom of Information and Protection of Privacy Act](#) are scheduled to come into force as of January 1, 2027.

In Newfoundland and Labrador, section 72 of ATIPPA, 2015 establishes:

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

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

While ATIPPA, 2015 uses the term common or integrated program or service, it is not defined in the legislation. Several other statutes define common or integrated program or service, including British Columbia's **Freedom of Information and Protection of Privacy Act** (FOIPPA BC), Alberta's **Protection of Privacy Act** (POPA), and Nova Scotia's **Freedom of Information and Protection of Privacy Act**.

Schedule 1 of British Columbia's [FIPPA](#) establishes:

- "common or integrated program or activity" means a program or activity that
- (a) provides one or more services through
 - (i) a public body and one or more other public bodies or agencies working collaboratively, or
 - (ii) one public body working on behalf of one or more other public bodies or agencies, and
 - (b) is confirmed by regulation as being a common or integrated program or activity;

Section 1(d) of Alberta's [POPA](#) states:

- (d) "common or integrated program or service", in relation to a public body, means a program or service planned, administered, delivered, managed, monitored or evaluated by
 - (i) the public body working collaboratively with one or more other public bodies, or
 - (ii) another public body working on behalf of
 - (A) the public body, or
 - (B) the public body and one or more other public bodies;

Section 3 of Nova Scotia's [FOIPOP](#), although passed in 2025, takes effect in 2027, states,

- "common or integrated program or activity" means a program or activity that
- (a) provides one or more services through
 - a public body and one or more other public bodies or partner agencies, working collaboratively, or

- one public body working on behalf of one or more other public bodies or partner agencies; and
- (b) is confirmed, in the manner provided by the regulations, as being a common or integrated program or activity

Since ATIPPA, 2015 was proclaimed in force over 10 years ago OIPC has received seven PIAs for common or integrated programs or services for review and feedback. This is a low number as there were likely more PIAs that should have been provided for review. This could be a reflection of confusion over what exactly qualifies as such a program or service. OIPC recommends that the term common or integrated program or service be defined in ATIPPA, 2015.

Section 72 currently requires that, during the development of a program or service, the head of a department or branch of the executive government shall submit to the minister responsible for this Act:

- (a) a privacy impact assessment for that minister's review and comment; or
- (b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.

While OIPC does not feel it would be beneficial or practical to require all public bodies to provide copies of all PIAs to our Office for review, we are sometimes unaware of the new programs and initiatives being undertaken by public bodies that involve the collection, use or disclosure of personal information. The ATIPP Office's annual reports provide a high-level snapshot, however does not generally provide details regarding the PIAs submitted to their Office. For example, their [2024-25 Annual Report](#) states that they received seven PIAs and 76 PPIAs during the fiscal year, for a total of 83 assessments. Furthermore, by the time an annual report has been issued it is usually too late to provide useful commentary.

In Alberta, certain circumstances require public bodies subject to POPA to submit privacy assessments to OIPC Alberta for review and comment. OIPC Alberta publishes a PIA registry on its [website](#). Since January 1, 2017, the office has accepted over 8,600 PIAs.

The Government of Canada has a [Directive on Privacy Practices](#) that applies to government institutions. Section 3 discusses objectives and expected results and addresses PIAs:

3.2.3 Privacy impact assessments (PIAs) are completed so that the privacy risks associated with programs and activities that use personal information for administrative purposes are identified, reviewed and updated, and appropriate mitigation measures implemented.

Section 4 of the policy establishes requirements for PIAs:

Ensuring the establishment of a PIA development and approval process, that:

- 4.1.11.1 Takes into consideration the responsibility within the institution for establishing PIBs; and
- 4.1.11.2 Is commensurate with the level of risk related to the privacy invasiveness of the institution's program or activities; and
- 4.1.12 Ensuring that a PIA is established for any program or activity that uses personal information for an administrative purpose;

Section 4.2 of the policy establishes the responsibilities of executives and senior officials, including responsibilities in regards to PIAs. This includes ensuring that PIAs are prepared and updated in accordance with [Appendix C: Standard on Privacy Impact Assessment](#), providing PIAs to TBS and the Office of the Privacy Commissioner (OPC), and ensuring that summaries of PIAs are published. For an example of published PIA summaries, see the Canada Revenue Agencies' [page](#).

Recommendations

Recommendation 2026-20-1: Require all public bodies to complete PIAs. The Minister responsible for the Act be required to maintain a comprehensive, up-to-date registry of PIAs, including a brief summary of all PIAs.

Recommendation 2026-20-2: Amend the Act to include a definition of "common or integrated program or service" similar to that of British Columbia.

Recommendation 2026-20-3: Include a provision in the Act that requires public bodies to submit a PIA to the Commissioner for review and comment upon the Commissioner's request.

Recommendation 2026-20-4: Add regulations that address critical PIA content, including requiring that PPIAs document why a full PIA is not recommended.

Mandatory Training

Training is a well-known administrative safeguard that helps protect personal information. Employees must be aware of what constitutes personal information as a first step as well as what protections should be in place to protect that information. While training alone can create foundational knowledge and proficiencies, awareness activities are required to keep messages top-of-mind among employees. Furthermore, different roles will require different training and should be tailored where appropriate. It is an ongoing effort that requires planning and resources, that, when done correctly, creates the foundation for a strong culture of privacy.

Section 64 of ATIPPA, 2015, states, in part:

- 64.(1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that
- (a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;
 - (b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and
 - (c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.

OIPC has issued guidance on [Reasonable Safeguards](#) that identifies three types of safeguards: administrative, technical and physical. Administrative safeguards include conducting regular staff training and awareness activities, as well as implementing policies and procedures that address staff training. OIPC's [Privacy Management Programs](#) guidance identifies training as a program control, stating, in part:

For an organization's training to be effective, it should:

- be mandatory for all new employees before they are exposed to or handle personal information or personal health information, and periodically thereafter;
- be tailored for the role of the employee;

- cover the policies and procedures established by the organization;
- be delivered in the most appropriate and effective manner, based on organizational needs;
- be tracked and documented; and
- circulate essential information to relevant employees as soon as practical if an urgent need arises.

Past reports and guidance issued by this Office have noted that employee training may already be considered an implied requirement, due to the obligation in section 64(1) that public bodies take reasonable steps to protect personal information. Although OIPC considers training to be important and arguably already implied by the statute, that implied obligation may not be widely recognized or understood among the large portion of public bodies.

This Office looked at how the matter is addressed in other Canadian jurisdictions and found that many provinces have policies, directives, standards, or administrative requirements for employee training rather than legislative requirements.

The Government of Canada requires mandatory training, however through a directive and not the [Privacy Act](#). The [Directive on Personal Information Requests and Correction of Personal Information](#) requires all employees of government institutions to receive training on obligations under the Privacy Act and related Treasury Board policy instruments. The policy also identifies topics that must be covered in training.

The [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) also does not contain a specific legislative requirement for training. However, Schedule 1 of PIPEDA contains the Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96. Principle 1 is accountability and it states, in part:

- 4.1.4 Organizations shall implement policies and practices to give effect to the principles, including ... (c) training staff and communicating to staff information about the organization's policies and practices; and ...

Further, the Privacy Commissioner of Canada has made it clear that training is an important expectation of accountable entities. For example, in a joint publication of the Offices of the

Information and Privacy Commissioners for Alberta and British Columbia, [Getting Accountability Right with a Privacy Management Program](#), training is identified as a key program control, stating, in part:

...

In order for a privacy management program to be effective, employees must be actively engaged in privacy protection. They need to be educated in privacy protection generally, and for those who handle personal information directly, they will need additional training specifically tailored to their roles. Training and education need to be recurrent, and the content of the program needs to be periodically revisited and updated to reflect changes.

...

For privacy training and education to be effective, it must:

- be mandatory for all new employees before they access personal information and periodically thereafter;
- cover the policies and procedures established by the organization;
- be delivered in the most appropriate and effective manner, based on organizational needs; and
- circulate essential information to relevant employees as soon as practical if an urgent need arises.

The Privacy Commissioner of Canada's guidance [Ten tips for avoiding complaints to the OPC](#) also identifies training as an important tool, stating,

2. Train staff about privacy

Put basic information on privacy protection responsibilities (and the designated privacy officer contact info) in tools and training for staff, especially customer service representatives and staff designing new customer products or forms, or new record keeping systems.

At a provincial level, section 36.2 of British Columbia's [Freedom of Information and Protection of Privacy Act](#) states, "The head of a public body must develop a privacy management program for the public body and must do so in accordance with the directions of the minister responsible for this Act." The Government of British Columbia's [Privacy Management and Accountability Policy](#) has an education and awareness section that establishes training requirements, including the responsibilities of Privacy Officer's to document this training. The Policy states,

Employees

- 2.4.1 Employees must complete training on the appropriate collection, use, disclosure, storage and disposal of Personal Information as prescribed by CIRMO, i.e., the IM117 course offered through the Public Service Agency. An exemption may be granted by CIRMO for extenuating circumstances.
- 2.4.2 Employees must complete the ministry-specific training or awareness activities referenced in s.2.4.4, s.2.4.7 and s.2.4.8, when applicable.
- 2.4.3 Employees, including Service Providers and volunteers, who collect or create Personal Information must complete privacy training developed by CIRMO, unless granted an exemption by CIRMO. The training is on the appropriate collection, use, disclosure, storage, access, retention and disposal of Personal Information, i.e., the FOIPPA Foundations course. This training must be completed prior to providing any service that involves Personal Information. Training referred to in s.2.4.1 may be applied towards this requirement (where it has been documented).
- 2.4.4 Employees may develop ministry-specific training to support this policy or compliance with FOIPPA in collaboration with MPOs and in keeping with ministry processes. Any such ministry-specific training must be submitted to CIRMO for review during development of the training.

Ministry Privacy Officers

- 2.4.5 MPOs must develop, maintain and review internal processes to ensure all Employees take the mandatory training or complete the awareness activities referred to in s.2.4.1 and s.2.4.2, as applicable.
- 2.4.6 MPOs must develop, maintain and review internal processes to:
 - ii. Document Service Providers and volunteers who have access to Personal Information; and
 - ii. Ensure that the Service Provider and volunteer training requirements referred to in s.2.4.3 are properly applied.
- 2.4.7 MPOs may, in collaboration with CIRMO, develop ministry-specific privacy training to support PMAP and/or privacy related matters.
- 2.4.8 MPOs must develop, maintain and review internal processes to ensure Employees who handle high risk or sensitive Personal Information within information systems or programs are aware of their privacy obligations. MPOs may use resources developed in collaboration with CIRMO or may use tools developed by CIRMO (once made available).
- 2.4.9 Once Ministry-specific training or awareness activities referred to in s.2.4.4, 2.4.7 and/or s.2.4.8 are developed, MPOs must ensure that the required activities are completed by all appropriate Employees within a timeline determined by the MPO.

Corporate Information and Records Management Office

2.4.10 CIRMO must develop training to support the appropriate collection, use, disclosure, storage and disposal of Personal Information (e.g., the privacy training referenced in s.2.4.1 and s.2.4.3).

Section 25 of Alberta's [Protection of Privacy Act](#) (POPA) requires public bodies to establish and implement a privacy management program that complies with the prescribed regulations. The [Protection of Privacy \(Ministerial\) Regulation](#) requires Privacy Management Programs to include, "6(d) mandatory training for employees of the public body about the obligations of those employees under the Act, with specified expiry periods after which retraining is required, ...".

When considering training, it is important to recognize that different positions will require different training. For example, janitorial staff will not require the same level of understanding as someone who handles personal information every day. However, they still have a role to play. For example, they should know if they can take pictures in the workplace, know what to do if they find paper with personal information on the floor or in the garbage, etc. Senior leadership may not directly handle personal information every day, however they may oversee programs that do, and must have a solid understanding of obligations. Entities would need to ensure appropriate training for the roles.

Recommendation

Recommendation 2026-21: Amend the Act to include a mandatory training requirement with clear obligations to track completion and ensure training is completed at regular intervals.

Additional Oversight or Enforcement Mechanisms

Terms of Reference Request: Consider whether additional oversight or enforcement mechanisms are needed.

As stated in our section regarding artificial intelligence, biometrics and surveillance, it is our belief that privacy and algorithmic impact assessments must be completed by public bodies

to ensure robust privacy protections are considered and implemented. This Office would like to see public bodies be mandated to complete PIAs and AIAs and that we be given the authority to obtain, review, and provide comments on them where programs collect, use or disclose sensitive personal information.

Effective privacy regulation should subject public bodies to enforcement mechanisms tailored to balance accountability with public interest. It is difficult to anticipate what government policies may be contemplated, but generally we encourage legislation where this Office would be notified of any programs that will involve the collection, use or disclosure of sensitive personal information with a mandate to issue recommendations that can pause unlawful government surveillance programs, data-sharing initiatives, or automated decision-making systems until compliance is confirmed.

Historically, this Office was consulted on draft legislation pursuant to section 112 of the Act which states:

112. (1) A minister shall consult with the commissioner on a proposed Bill that could have implications for access to information or protection of privacy, as soon as possible before, and not later than, the date on which notice to introduce the Bill in the House of Assembly is given.
- (2) The commissioner shall advise the minister as to whether the proposed Bill has implications for access to information or protection of privacy.
- (3) The commissioner may comment publicly on a draft Bill any time after that draft Bill has been made public.

Unfortunately, the previous government decided to discontinue the practice of providing the text of draft bills to this Office for review, and it has not been re-implemented by the current government. Former Commissioner Harvey provided commentary on that issue in a [Special Report to the Legislature](#). While we do continue to be consulted on the broad strokes of draft bills, the high-level policy purpose rarely triggers any concerns nor provides an opportunity for meaningful comment. Our experience is that the specific words of a statute - what is being enabled or required by the words in a draft bill - is where the privacy and access to information risks emerge. Unless we can actually review and comment on those, as we previously did, the consultation process has limited utility.

We believe the current provision at section 112 already requires that level of consultation. If government believes that it is not sufficiently clear in that regard, we ask that it be amended in a way that will facilitate a return of the previous practice which was beneficial to all.

Recommendation

Recommendation 2026-22: If government considers the consultation requirements in section 112 to be insufficiently clear to facilitate the provision of draft bills to the Commissioner for review, section 112 should be amended to expressly require it.

PUBLIC BODY PRACTICES AND ACCOUNTABILITY – OTHER SIGNIFICANT ISSUES

Duty to Document

The Duty to Document has been defined by former B.C. Information and Privacy Commissioner David Loukidelis as “a legal duty requiring public servants to adequately document specified decisions and actions.” We expect that many Newfoundlanders and Labradorians would be surprised that no such requirement broadly exists in law already. Not only is it not legally entrenched here, among all jurisdictions only British Columbia has formally implemented a Duty to Document.

Recommendation #15 of Justice LeBlanc’s final report on the Commission of Inquiry Respecting the Muskrat Falls Project referenced the Duty to Document:

Government should legislate and fully implement a “duty to document” policy within six months of the submission of this Report. The duty to document should also apply to Crown corporations and agencies.

The Report of the 2014 Statutory Review of ATIPPA recommended implementation of a Duty to Document, as an amendment to the Management of Information Act (MOIA), with compliance to be overseen by the Information and Privacy Commissioner. As with the Muskrat Falls Report, Government accepted the recommendation to implement a Duty to Document from the Report of the 2014 Statutory Review of ATIPPA as well but, unlike most other recommendations, decided not to immediately act upon it.

A Duty to Document provision and a related offence provision were added to the **House of Assembly Accountability, Integrity and Administration Act** in 2017:

21.1 The commission, officers and staff of the House of Assembly service shall be responsible and accountable for ensuring that all advice, deliberations, decisions and recommendations of the commission that result from formal or informal meetings of the members of the commission are properly documented in accordance with the Records Management Policy of the House of Assembly.

[...]

66.(1) A person who fails to comply with section 21.1 is guilty of an offence.

(2) A person having a duty to document decisions and maintain records of the commission, the speaker, the clerk or staff member of the House of Assembly service and a person who without lawful authority destroys documentation recording decisions of the commission, the speaker or the clerk, or the advice and deliberations leading up to those decisions, is guilty of an offence.

(3) A person who is guilty of an offence under subsection (1) or (2) is liable on summary conviction to a fine of not more than \$10,000 or to imprisonment up to 6 months.

These new provisions were added as a result of a [Report of the Members' Compensation Review Committee from November 2016](#). In addition to reporting on MHA compensation, that report identified a number of shortcomings in the operation of the House of Assembly Management Commission, and among other things it made recommendations regarding documentation of decisions and public disclosure (beginning at page 102 of that Report).

The [Management of Information Act](#) (MOIA), requires “public bodies” (defined differently than in ATIPPA, 2015 and omitting “local public bodies” and “local government bodies”) to “develop, implement and maintain a record management system for the creation, classification, retention, storage, maintenance, retrieval, preservation, protection, disposal and transfer of government records.” The **Management of Information Act** does not feature an independent oversight body, however, so there is no basis upon which to assess whether the approach to creation of records has been implemented or adhered to.

Missing from the Newfoundland and Labrador **Management of Information Act** are provisions for ensuring that an appropriate system is in place within the government body for creating and maintaining, in accordance with applicable directives or guidelines, government information that is an adequate record of that government body's decisions.

Chair Orsborn, in the Report of the 2020 Statutory Review of ATIPPA, reviewed the history of various calls for implementation of a statutory duty to document. He closed that section of his Report with this: “I make only one comment – enough time has passed.”

[Bill 22](#) was introduced into the legislature in 2023. It proposed to amend MOIA in a way that was described as implementing a duty to document. Former Commissioner Michael Harvey issued a [public statement](#) about the Bill in accordance with section 112(3) of ATIPPA, 2015 in which he expressed the view that the Bill did not accomplish the intent of a legislated duty to document. The Bill did not proceed past second reading.

OIPC’s position is consistent with the recommendation of the 2014 Statutory Review Committee, that a Duty to Document requirement should be added, ideally to the **Management of Information Act**. We recommend that that this be accomplished through an amendment to MOIA alongside amendments to ATIPPA, 2015 to enable the Commissioner to have oversight of the Duty to Document.

Recommendations

Recommendation 2026-23-1: Amend the Management of Information Act to legislate a Duty to Document for entities subject to that legislation, providing for OIPC oversight.

Recommendation 2026-23-2: Consider whether to broaden the scope of public bodies to which the Duty to Document would apply, to all public bodies subject to ATIPPA, 2015 except those that are subject to the Towns and Local Service Districts Act.

Publication Schemes, Information Directories and Proactive Disclosure

The [Final Report from the 2020 ATIPPA Statutory Review Committee](#) made a number of recommendations involving Publication Schemes, Information Directories and Proactive Disclosure. We agree with recommendations.

OIPC's submission to the ATIPPA Statutory Review Committee 2020 contains a detailed overview of publication schemes beginning on page 59, which may be of assistance to this Review Committee by providing additional context on this issue.

Public bodies need to know what records they have and where they are located if they are to meet the access to information requirements of the Act. Similarly, all public bodies are subject to Part III of ATIPPA, 2015 (the protection of personal information). To comply with the privacy provisions of ATIPPA, 2015, public bodies must know what information they have, where it is stored, how it moves and how long it is retained. The terms of reference for this 2026 review also include discussions of privacy management programs. A key component of such a program is an inventory of personal information held by a public body.

Requiring public bodies to develop and publish a publication scheme should not be an onerous task, as it should already have familiarity with the records in its custody or control. In January 2016, OIPC issued guidance titled "[Publication Scheme Template](#)", so OIPC's expectations and opinions on publication schemes should not be a surprise to public bodies.

On March 15, 2024, the ATIPP Office posted its response to ATIPP/1/2023, an access request for "information relating to ATIPP requests submitted to government departments from January 1, 2022 to June 30, 2023." The response to this request provided an opportunity for OIPC to analyze requests made to various government departments, look for trends and develop guidance and training to assist ATIPP Coordinators. OIPC noted that many of the access requests were complicated and involved very specific matters. We do note that the request was limited to government departments and does not reflect the work of all ATIPP Coordinators, excluding, for example, municipalities, healthcare entities and agencies.

Further, the released record reflects general access requests and not those that were for personal information.

OIPC has a number of observations from this review.

Proactive Disclosure

In reviewing the access requests, there are a number of repeated requests that could be addressed through proactive disclosure. For example:

- Communications Materials
 - A copy of the briefing book used by the Minister in the House of Assembly
 - List of all briefing materials provided to Briefing Binder for the Estimates Committee
 - Transition Binders
 - Speaking Notes, Decision/Direction notes, Information Notes, Q&As, etc.
- Expense Claims
 - Detailed list of expenses claimed
 - Total costs of trips (especially interested in out-of-country travel)
 - Journey Authorization Forms
- Reports
 - When government announces that it has commissioned a report, and/or that the report has been submitted, copies are generally requested through access requests.

Proactive disclosure may reduce the number of access requests received, and it will definitely contribute to the public body's openness and transparency efforts. The Review Committee should strongly consider any previous recommendations made for proactive disclosure. For example, if information is removed from documents before posting, best practice would be to inform individuals of this fact. For example, if a decision is made to exclude particular sections of posted briefing notes, note this fact.

Publication Schemes

There were also a number of departments that had a high number of responses that “Records Do Not Exist”. We suggest that departments review their responses to access requests for trends, which may then lead to clarifications on their websites. For example:

- Municipal and Provincial Affairs – what type of records are held by the department and what types are held by towns?
- Department of Health and Community Services – what types of records are held by the department, and what types are held by NL Health Services?

It may be beneficial for departments that receive a number of access requests for records they do not hold to consider telling people this up front to prevent the access request coming to them in the first place.

ATIPPA, 2015 "SCHEDULE A" REVIEW

Terms of Reference Request: Review the list of provisions in Schedule A to determine the necessity of their continued inclusion.

Schedule A is tied to section 7 of ATIPPA, 2015, which states:

7. (1) Where there is a conflict between this Act or a regulation made under this Act and another Act or regulation enacted before or after the coming into force of this Act, this Act or the regulation made under it shall prevail.
- (2) 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.
- (3) When the House of Assembly is not in session, the Lieutenant-Governor in Council may by order amend Schedule A, but the order shall not continue in force beyond the end of the next sitting of the House of Assembly.

The 2020 Statutory Review of ATIPPA, conducted by Chair Orsborn, made some recommendations regarding Schedule A of ATIPPA, 2015. The recommendations impacted the following sections of Schedule A:

- (f) section 8.1 of the **Evidence Act**;
- (h) subsection 5(1) of the **Fish Inspection Act**;
- (i) section 4 of the **Fisheries Act**;
- (j.01) section 31 of the **Hydro Corporation Act, 2024**;
- (j.1) section 21 of the **Innovation and Business Investment Corporation Act**;
- (l.1) section 23 of the **Oil and Gas Corporation Act**;
- (t) section 19 of the **Workplace Health, Safety and Compensation Act, 2022**.

Our position and commentary on these specific sections of Schedule A are located in [Appendix A](#) of this submission. OIPC agrees with all the recommendations for these sections noting that section 5.4 of the **Energy Corporation Act** is now section 31 of the **Hydro Corporation Act** and that section 18 of the **Workplace Health, Safety and Compensation Act** is now section 19 of the **Workplace, Health, Safety and Compensation Act, 2022**.

The remaining sections of Schedule A are as follows:

- (a) sections 64 to 68 of the **Adoption Act, 2013**;
- (b) sections 33 and 34 of the **Adult Protection Act, 2021**;
- (b.1) subsection 30(2) of the **Auditor General Act, 2021**;
- (c) section 115 of the **Canada-Newfoundland and Labrador Atlantic Accord Implementation and Offshore Renewable Energy Management Newfoundland and Labrador Act**;
- (d) sections 90 to 96 of the **Children, Youth and Families Act**;
- (g) subsection 24(1) of the **Fatalities Investigations Act**;
- (j) sections 173, 174 and 174.1 of the **Highway Traffic Act**;
- (j.2) section 6 and paragraph 7(1)(b) of the **Interpersonal Violence Disclosure Protocol Act**;
- (k) section 15 of the **Mineral Act**;
- (l) section 16 of the **Mineral Holdings Impost Act**;
- (m) subsection 13(3) of the **Order of Newfoundland and Labrador Act**;
- (m.1) sections 10 and 15 of the **Patient Safety Act**;
- (n) sections 153, 154 and 155 of the **Petroleum Drilling Regulations**;
- (o) sections 53 and 56 of the **Petroleum Regulations**;
- (p) [Rep. by 2018 cl-7.1 s24]
- (q) section 12 and subsection 96.2(2) of the **Schools Act, 1997**;

- (r) sections 19 and 20 of the **Securities Act**;
- (s) section 13 of the **Statistics Agency Act**; and

We have no comments on any of the above sections, except for section (q) which references section 12 and subsection 96.2(2) of the [Schools Act, 1997](#). Section 12 of the **Schools Act, 1997** addresses student records as follows:

- 12.(1) A student record shall be maintained for each student in the manner required by a policy directive of the minister.
- (2) Except as provided in this section a student record may only be reviewed by
 - (a) the parent of the student; or
 - (b) the student, if the student is 19 years of age or older,to whom that student record pertains.
- (3) A parent or student, if the student is 19 years of age or older, shall review the student record at a time and with a person designated by the department or the conseil scolaire and receive an explanation and interpretation of information in the student record from that person.
- (4) A parent or student, if the student is 19 years of age or older, who is of the opinion that the student record contains inaccurate or incomplete information may request the principal to review the matter.
- (5) A student record may be used by the principal and teachers of a school and by employees of the department or the conseil scolaire to assist in the instruction of the student to whom that student record pertains.
- (6) Without the written permission of the parent of a student, or the student if the student is 19 years of age or older,
 - (a) a student record shall not be admissible in evidence in a trial, inquiry, examination, hearing or other proceeding except to prove the establishment, maintenance, retention or transfer of that student record; and
 - (b) a person shall not be required to give evidence respecting the content of the student record in a trial, inquiry, examination, hearing or other proceeding.
- (7) Notwithstanding subsections (1) to (6), a principal may use a student record to prepare information or a report
 - (a) required under this Act; and
 - (b) when requested in writing by a parent, or where a student is 19 years of age or older, the student or former student, for
 - (i) an educational institution, or

(ii) an application for employment.

- (8) This section shall not prevent the use of a report based upon a student record by the principal of a school attended by that student, the department or the conseil scolaire, for the purpose of a disciplinary proceeding commenced by the principal respecting the conduct of that student or a prosecution of an offence under this Act.
- (9) An action shall not lie against a person who contributes test results, evaluations or other information to a student record where the person acted in good faith within the scope of the person's duties.

We suggest that this section be reviewed to determine if Schedule A should include all of section 12, or just subsections of section 12. Our concern is that ATIPPA, 2015 contains no age restrictions on access to records but section 12 has a restriction of access to "parents of the student" or "the student, if the student is 19 years of age or older."

Section 96.2(2) of the **Schools Act, 1997** states as follows:

- (2) Notwithstanding subsection (1), the minutes of a closed meeting shall not be available to the public.

As ATIPPA, 2015 already contains provisions excepting access to records of closed meetings, Our position is that this provision in Schedule A is redundant and should be removed.

Recommendations

Recommendation 2026-24-1: Review section 12 of the **Schools Act, 1997** to determine if all of section 12 should be included in Schedule A, or just subsections of section 12.

Recommendation 2026-24-2: Remove section 96.2(2) of the **Schools Act, 1997** from Schedule A.

Appendix A – OIPC'S Consideration of the 2020 Statutory Review Recommendations

The table begins on the following page. The remainder of this page is intentionally left blank.

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
1	THE ATIPP COORDINATOR (Administrative)	That the head of each public body provide each designated ATIPP coordinator with a formal mandate letter.	No Comment.	
1	THE ATIPP COORDINATOR (Administrative)	That the Classification and Organization Design section of Treasury Board develop a job description and classification for the position of full-time	No Comment.	
1	THE ATIPP COORDINATOR (Administrative)	That each coordinator sign an oath/affirmation of confidentiality addressing their particular obligations as coordinators.	No Comment.	
1	THE APPLICANT	That the Act be amended to: Require the full name and contact information of the applicant for all requests. [Appendix K, s. 11(2)(a.1)]	Agree.	
2	THE APPLICANT	That the Act be amended to: Make it clear that the anonymity of an applicant continues to apply following the final response to the applicant. [Appendix K, s. 12(4)]	Agree except if the matter should proceed to Court.	
2	THE APPLICANT	That the Act be amended to: 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. [Appendix K, s. 11.1]	Partially Agree. While identity verification is appropriate, clarification requests are subjective and should not extend timelines. The proposed 30 day period could undermine the 20 business day response requirement and may be used to delay access requests.	
2	THE APPLICANT	That the Act be amended to: Stop the clock on time limits for final responses while waiting for an applicant's response to a request for clarification or identity verification. [Appendix K, s. 11.1(3)]	Disagree. The ability to request time extensions from the Commissioner already exists. The proposed 30 day period could undermine the 20 business day response requirement and may be used to delay access requests.	
2	THE REQUEST PROCESS - Fees and Costs	That the Act be amended to: Allow public bodies 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. [Appendix K, s. 8(3), s. 25]	Disagree.	
2	THE REQUEST PROCESS - Fees and Costs	That the Act be amended to: Allow public bodies to charge fees per page for physical reproduction of records in excess of 100 pages. [Appendix K, s.	Disagree.	
2	THE REQUEST PROCESS - Fees and Costs (Administrative)	That the responsible minister revise the current cost schedule to reflect the recommendations in this report.	Disagree.	
2-3	THE REQUEST PROCESS - Record Format	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.) [Appendix K, s. 20(6) and (7)]	No amendment needed as section 20 of the Act already supports this.	
3	THE REQUEST PROCESS - Record Format (Administrative)	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.	Agree.	
3	THE REQUEST PROCESS - Transfer of Requests	That the Act be amended to expand the window for transferring requests between public bodies to 10 days. [Appendix K, s. 14(1)]	Agree.	
3	THE REQUEST PROCESS - Transfer of Requests (Administrative)	That concurrently with the transfer of an access request to another public body, the transferring coordinator notify the ATIPP Office of the transfer.	No Comment.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
3-4	THE REQUEST PROCESS - Advisory Response	That the Act be amended to remove the requirement for advisory responses. [Appendix K, s. 15]	Agree.	
4	THE REQUEST PROCESS - Advisory Response (Administrative)	That acknowledgement letters be automatically generated and sent to applicants when a coordinator confirms receipt of a request.	No Comment.	
4	THE REQUEST PROCESS - Disregarding a Request	That the Act be amended to: Extend the period in which to apply for a disregard to 10 days. [Appendix K, s. 21(1)]	Agree.	Page 45
4	THE REQUEST PROCESS - Disregarding a Request	That the Act be amended to: Remove the ability to apply to disregard a request on the basis of unreasonable interference with the public body. [Appendix K, s. 21(1)(a)]	No Comment.	
4	THE REQUEST PROCESS - Disregarding a Request	That the Act be amended to: Stop the clock on time limits for final responses while waiting for the commissioner's approval of a disregard application. [Appendix K, s. 21(3)]	Disagree. Our position is that stopping the clock creates a potential for misuse.	
4	THE REQUEST PROCESS - Disregarding a Request	That the Act be amended to: 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. [Appendix K, s. 5(2)(a), s. 21.1]	Disagree. A public body should never been given the ability to approve their own disregards. ATIPPA already has provisions for a public body to direct an applicant to public information. The OIPC can approve a disregard for unidentifiable applicants.	
4	THE REQUEST PROCESS - Disregarding a Request (Administrative)	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.	No Comment.	
5	THE REQUEST PROCESS - Vexatious Applicants	That the Act be amended to: 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. [Appendix K, s. 21.2]	Disagree. Public bodies should be required to apply to court to have an applicant declared vexatious, with the Commissioner retaining the authority to intervene in the court matter.	
5	THE REQUEST PROCESS - Vexatious Applicants	That the Act be amended to: Allow an applicant to appeal a vexatious applicant declaration to the court and allow the court to make an appropriate order. [Appendix K, s. 54.1, s. 60(4)]	Disagree. See above.	
5	THE REQUEST PROCESS - Time Limits and Extensions	That the Act be amended to: 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. [Appendix K, s. 23.1]	Disagree. ATIPPA, 2015 already provides a mechanism to extend response timelines where justified. Available statistics indicate that public bodies are generally able to respond within the existing framework.	Page 40
5	THE REQUEST PROCESS - Time Limits and Extensions	That the Act be amended to: 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. [Appendix K, s. 23.1]	Disagree. This proposal could place applicants in a difficult position and create pressure to agree to delays requested by public bodies due to the power imbalance between the parties. The Act already contains an established extension process that provides appropriate safeguards and oversight.	Page 40
5	THE REQUEST PROCESS - Time Limits and Extensions (Administrative)	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	Disagree. The ATIPP Office can already require this from core government by policy. It would be an unfair burden to other public bodies.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
6	INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY ISSUES (Administrative)	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.	No comment.	
6	INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY ISSUES (Administrative)	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.	No Comment.	
6	INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY ISSUES (Administrative)	That OCIO and the ATIPP Office investigate and take steps as are appropriate to provide coordinators with pre-authorized, continuous access to frequently searched email accounts.	No Comment.	
6	INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY ISSUES (Administrative)	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.	No comment.	
6	INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY ISSUES (Administrative)	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.	No Comment.	
6	INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY ISSUES (Administrative)	That each public body not subject to the Management of Information Act review the content of and compliance with any existing guidelines for the disposal of transitory emails, or develop guidelines forthwith.	No Comment.	
6-7	EXCEPTIONS TO ACCESS - CABINET CONFIDENCES	That the Act be amended to remove "decisions" from the definition of "Cabinet record". [Appendix K, s. 27(1)(e)]	Agree.	
7	EXCEPTIONS TO ACCESS - Local Public Body Confidences	That the Act be amended to: Make it clear that privileged meetings of a municipal council committee have the same exceptions to disclosure as privileged meetings of the council. [Appendix K, s. 28(1)(c)]	Subsequent legislative changes have addressed this issue for most municipalities. Section 41(1) of the Towns and Local Service Districts Act clarifies that the closed meeting provisions apply to both council and committee meetings. For municipalities operating under separate legislation (City of St. John's Act, the City of Mount Pearl Act, and the City of Corner Brook Act), similar language could be adopted to provide clarity and limit closed meetings to specified purposes, supporting transparency.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
7	EXCEPTIONS TO ACCESS - Local Public Body Confidences	That the Act be amended to: Remove regulation-making authority relating to privileged meetings of a local public body or committee. [Appendix K, s. 116(f)]	See above.	
7	EXCEPTIONS TO ACCESS - Solicitor-Client Privilege	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. [Appendix K, s. 97]	Partially Agree. Clarifying the Commissioner's authority to require production of records subject to solicitor-client privilege would resolve existing uncertainty and support effective oversight. Beyond this clarification, no additional legislative changes are required.	Page 5
7	EXCEPTIONS TO ACCESS - Solicitor-Client Privilege	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. [Appendix K, s. 98]	Disagree. The Commissioner must be able to review records claimed to be subject to solicitor-client privilege to assess whether the claim is valid. Removing this authority would undermine independent oversight and accountability.	Page 5
7	EXCEPTIONS TO ACCESS - Solicitor-Client Privilege (Suggestion)	That public bodies support claims of solicitor-client privilege with a solicitor's affidavit and a listing and description of each document.	Agree.	
8	EXCEPTIONS TO ACCESS - Settlement Privilege	That the Act be amended to include settlement privilege in subsection 30(2). [Appendix K, s. 30(2)]	Disagree.	Page 14
8	EXCEPTIONS TO ACCESS - Confidential Evaluations	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. [Appendix K, s. 32(f)]	Agree.	
8	EXCEPTIONS TO ACCESS - Workplace Investigations	That the Act be amended to: Extend the definition of "workplace investigation" to include others holding a position within a public body. [Appendix K, s. 33(1)(c)(i) and (iii)]	Disagree. Our submission sets out the OIPC's position re section 33.	Page 15
8	EXCEPTIONS TO ACCESS - Workplace Investigations	That the Act be amended to: 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 complainant or respondent, or otherwise where in the public interest. [Appendix K, s. 33(2) and (3)]	Partially Agree. Our submission sets out the OIPC's position re section 33.	Page 15
8	EXCEPTIONS TO ACCESS - Workplace Investigations	That the Act be amended to: 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. [Appendix K, s. 33(4)]	Agree	Page 15
9	EXCEPTIONS TO ACCESS - Workplace Investigations	That the Act be amended to: Remove the House of Assembly Act and House of Assembly Accountability, Integrity and Administration Act inquiries from s. 33. [Appendix, s. 33(1.1)]	Disagree.	Page 15
9	EXCEPTIONS TO ACCESS - Workplace Investigations	That the Act be amended to: Allow the head of a public body to refuse access to information relating to workplace conduct provided in confidence, including opinions about another individual. [Appendix K, s. 33(5)]	Disagree. Our submission sets out the OIPC's position re section 33.	Page 15
9	EXCEPTIONS TO ACCESS - Intergovernmental Relations	That the Act be amended to extend the intergovernmental relations exception to all Indigenous self-governing bodies. [Appendix K, s. 2(l.1), s. 34(1)(a)(v), s. 34(1)(b)]	Agree with respect to all recognized Indigenous self-governing bodies.	
9	EXCEPTIONS TO ACCESS - Conservation	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. [Appendix K, s. 36(b)]	Agree.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
9	EXCEPTIONS TO ACCESS - Third Party Commercial Interests	That the Act be amended to: Remove the requirement that information has to have been supplied in confidence from the exception for disclosure harmful to third parties' business interests. [Appendix K, s. 39]	Disagree.	Page 25
9	EXCEPTIONS TO ACCESS - Third Party Commercial Interests	That the Act be amended to: Provide a mandatory exception for trade secrets. [Appendix K, s. 39(1)(a)]	Disagree.	Page 25
10	EXCEPTIONS TO ACCESS - Third Party Commercial Interests	That the Act be amended to: Provide a 20-year sunset clause on third-party business information. [Appendix K, s. 39(4)]	Agree.	Page 25
10	EXCEPTIONS TO ACCESS - Third Party Commercial Interests	That the Act be amended to: Make the exception for disclosure harmful to third parties' business interests subject to the public interest override. [Appendix K, s. 9(2)]	Agree.	Page 25
10	EXCEPTIONS TO ACCESS - Third Party Notification	That the Act be amended to: Allow public bodies to consult with third parties while considering requests for information the release of which might be harmful to their interests. [Appendix K, s. 19(1)]	Disagree.	Page 25
10	EXCEPTIONS TO ACCESS - Third Party Notification	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. [Appendix K, s. 19(5)(c)]	Agree.	Page 25
10	EXCEPTIONS TO ACCESS - Information Technology Security	That the Act be amended to provide a discretionary harm-based exception to access for information technology security information. [Appendix K, s. 31.1]	Disagree.	Page 37
10	EXCEPTIONS TO ACCESS - Information Technology Security (Administrative)	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.	No comment.	
11	EXCEPTIONS TO ACCESS - Testing Procedures and Audits	That the Act be amended to provide a discretionary harm-based exception to access for test-related information. [Appendix K, s. 5(1)(f), s. 41.1]	Agree.	
11	PUBLIC INTEREST OVERRIDE	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. [Appendix K, s. 9, s. 33(3)(b)]	Agree.	Page 36
11	SUNSET CLAUSES	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. [Appendix K, s. 38(2), s. 39(4)]	Agree.	
12	SUBMISSIONS OF THE NEWFOUNDLAND AND LABRADOR VETERINARY MEDICAL ASSOCIATION	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. [Appendix K, s. 5(1)(n)]	Agree.	
12	SUBMISSIONS OF THE OFFICE OF THE SPEAKER OF THE HOUSE OF ASSEMBLY - The "Next Sitting" of the House of Assembly	That the Act be amended to: Provide the Lieutenant-Governor-in-Council with the authority to recommend additions to Schedule B. [Appendix K, s. 4]	Agree.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
12	SUBMISSIONS OF THE OFFICE OF THE SPEAKER OF THE HOUSE OF ASSEMBLY - The "Next Sitting" of the House of Assembly	That the Act be amended to: Require the Selection Committee to provide no more than three candidate names to the Speaker when choosing a new commissioner. [Appendix K, s. 85(5)]	Agree.	
12	SUBMISSIONS OF THE OFFICE OF THE SPEAKER OF THE HOUSE OF ASSEMBLY - The "Next Sitting" of the House of Assembly	That the Act be amended to: Give the formal responsibility for bringing forward the resolution naming a new commissioner to the government House Leader. [Appendix K, s. 85(6) and (7)]	Agree.	
12	SUBMISSIONS OF THE OFFICE OF THE SPEAKER OF THE HOUSE OF ASSEMBLY - The "Next Sitting" of the House of Assembly (Suggestion)	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.	Agree.	
13	SUBMISSIONS OF THE OFFICE OF THE SPEAKER OF THE HOUSE OF ASSEMBLY - The "Next Sitting" of the House of Assembly (Suggestion)	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.	Agree.	
13	SUBMISSIONS OF THE STATUTORY OFFICES OF THE HOUSE OF ASSEMBLY - Office of the Auditor General	That the Act be amended to: Make clear that the exception to disclosure for statutory office records extends to those offices' audit functions. [Appendix K, s. 41(c)]	Agree.	
13	SUBMISSIONS OF THE STATUTORY OFFICES OF THE HOUSE OF ASSEMBLY - Office of the Auditor General	That the Act be amended to: Make the Office of the Auditor General subject to ATIPPA, 2015. [Appendix K, s. 2(x)(v.1)]	Agree.	
13	OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER	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. [Appendix K, s. 103.1]	Agree.	Page 50
13	OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER - The Office of the Information and Privacy Commissioner as a Public Body	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. [Appendix K, s. 51.1]	Agree.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
14	OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER - Compellability of OIPC Personnel as Witnesses	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. [Appendix K, s. 99(3)]	Disagree.	
14	OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER - OIPC Investigations and Section 8.1 of the Evidence Act	That the Act be amended to repeal section 101. [Appendix K, s. 101]	Disagree. Section 101 should remain in ATIPPA, 2015	
14	MUNICIPALITIES	That the Act be amended to: Provide that only one person can be designated as the head of a local public body. [Appendix K, s. 109(1), (2)(a), (3) and (4)]	Agree.	
14	MUNICIPALITIES	That the Act be amended to: 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. [Appendix K, s. 110(3) and (4)]	Agree.	
14-15	MUNICIPALITIES (Administrative)	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.	No Comment. Applicable legislation is now called the Towns and Local Service Districts Act.	
15	MUNICIPALITIES (Administrative)	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.	No Comment.	
15	RECOMMENDATIONS 4 AND 16 OF THE MUSKRAT FALLS INQUIRY	That the Act be amended to: Provide that a public inquiry is not a public body for ATIPP purposes. [Appendix K, s. 2(x)(x)]	Agree.	
15	RECOMMENDATIONS 4 AND 16 OF THE MUSKRAT FALLS INQUIRY	That the Act be amended to: Include s. 28 of the Public Inquiries Act, 2006 in Schedule A. [Appendix K, Schedule A (o.1)]	No Comment.	
15	RECOMMENDATIONS 4 AND 16 OF THE MUSKRAT FALLS INQUIRY (Suggestion)	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 Comment.	
15-16	PUBLICATION SCHEMES, INFORMATION DIRECTORIES AND PROACTIVE DISCLOSURE - Proactive Disclosure	That the Act be amended to: Require the creation of publication schemes by all public bodies other than small municipalities and others exempted by regulation. [Appendix K, s. 111]	Agree.	Page 98
16	PUBLICATION SCHEMES, INFORMATION DIRECTORIES AND PROACTIVE DISCLOSURE - Proactive Disclosure	That the Act be amended to: Require public bodies other than local public bodies to develop and publish categories of records and information that will be published routinely. [Appendix K, s. 111.1]	Agree.	Page 98

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
16	PUBLICATION SCHEMES, INFORMATION DIRECTORIES AND PROACTIVE DISCLOSURE - Proactive Disclosure	That the Act be amended to: 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. [Appendix K, s. 111.1(5)]	Agree.	Page 98
16	PUBLICATION SCHEMES, INFORMATION DIRECTORIES AND PROACTIVE DISCLOSURE - Proactive Disclosure	That the Act be amended to: Allow the commissioner to comment on and recommend improvements to publication schemes and proactive disclosure. [Appendix K, s. 95(1)(i)]	Agree.	Page 98
16	PUBLICATION SCHEMES, INFORMATION DIRECTORIES AND PROACTIVE DISCLOSURE - Proactive Disclosure	That the Act be amended to: Delay the coming into effect of the publication scheme and proactive disclosure provisions until January 1, 2023.	Agree and date must be updated.	Page 98
16	PUBLICATION SCHEMES, INFORMATION DIRECTORIES AND PROACTIVE DISCLOSURE - Proactive Disclosure (Administrative)	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.	Agree.	Page 98
16	PROTECTION OF PRIVACY	That the Act be amended to require a public body to develop and publish policies and procedures for the protection of personal information. [Appendix K,	Agree.	
16-17	PROTECTION OF PRIVACY	That the Act be amended to: Define "common or integrated program or service". [Appendix K, s. 2(e.1)]	Partially Agree. We recommend that a definition of "common or integrated program or service" similar to that of B.C. be added to the Act	Page 84
17	PROTECTION OF PRIVACY	That the Act be amended to: 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. [Appendix K, s. 2(w), s. 72.1]	Agree; however, also include a provision in the Act that requires public bodies to submit a PIA to the Commissioner for review and comment upon the Commissioner's request.	Page 84
17	PROTECTION OF PRIVACY	That the Act be amended to: Specify that the commissioner has the authority to monitor compliance with the requirement to conduct privacy assessments and to make recommendations for improvement. [Appendix K, s. 95(1)(h)]	Agree.	Page 84
17	PROTECTION OF PRIVACY (Administrative)	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.	Agree.	
17	PROTECTION OF PRIVACY (Suggestion)	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.	Agree.	
17	PROTECTION OF PRIVACY (Suggestion)	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.	Agree.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
17	PROTECTION OF PRIVACY - Information Sharing Agreements (Administrative)	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	Agree.	
17-18	PROTECTION OF PRIVACY - Artificial Intelligence	That the Act be amended to: Define "automated decision system". [Appendix K, s. 2(a.2)]	Agree that there should be a definition of "automated decision system", however, we have not proposed specific wording.	
18	PROTECTION OF PRIVACY - Artificial Intelligence	That the Act be amended to: 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. [Appendix K, s. 2(a.1)]	Agree that there should be a definition of "algorithmic impact assessments" however, we have not proposed specific wording.	
18	PROTECTION OF PRIVACY - Artificial Intelligence	That the Act be amended to: Require that public bodies notify the commissioner when developing a program or service using automated decision systems. [Appendix K, s. 95(1)(f) and (g)]	Partially Agree; however, instead of notifying the commissioner, we recommend that the Act include a requirement that government publish a registry of AI impact assessments. The Commissioner should be entitled to require that a public body provide a particular AI impact assessment for review upon request, and the Commissioner should be enabled through clear statutory language to comment on any implications for the use of AI.	Page 53
18	PROTECTION OF PRIVACY - Artificial Intelligence	That the Act be amended to: Require public bodies to keep records of the decision-making processes of automated decision systems. [Appendix K, s.	Agree.	Page 53
18	PROTECTION OF PRIVACY - Artificial Intelligence	That the Act be amended to: Include monitoring and commenting on automated decision systems in the general powers and duties of the commissioner. [Appendix K, s. 72.3(4)]	Agree.	Page 53
18	PROTECTION OF PRIVACY - Privacy Breach Reporting	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. [Appendix K, s. 64]	Agree.	
18	PROTECTION OF PRIVACY - Privacy Breach Reporting (Administrative)	That all public bodies report privacy breaches to the ATIPP Office as well as to the OIPC.	No Comment.	
19	PROTECTION OF PRIVACY - Prospective and Third Party Privacy Complaints	That the Act be amended to: Allow complainants to file prospective complaints about privacy breaches. [Appendix K, s. 73(1) and (2)]	Agree. This is already allowed in PHIA under section 66(3).	
19	PROTECTION OF PRIVACY - Prospective and Third Party Privacy Complaints	That the Act be amended to: Remove the requirement for individual consent to the filing of a privacy complaint. [Appendix K, s. 73(1) and (2)]	Agree. This is already allowed in PHIA under section 66(3).	
19	PROTECTION OF PRIVACY - Anonymity of Privacy Complaints	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. [Appendix K, s. 73(6), (7) and (8)]	Agree.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
19	POLITICAL PARTIES AND PERSONAL INFORMATION (Administrative)	That government proceed expeditiously with the development of a regulatory and oversight regime covering the collection, use and disclosure of personal information by registered political parties.	Agree.	Page 64
20	ALUMNI ENGAGEMENT	That the Act be amended to: Allow post-secondary educational bodies to use personal information in alumni records for outreach and engagement purposes. [Appendix K, s. 67]	No Comment.	
20	ALUMNI ENGAGEMENT	That the Act be amended to: Allow alumni to request that their personal information cease to be used for outreach and engagement activities. [Appendix K, s. 67(2)(c)]	No Comment.	
20	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Parties to a Complaint	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. [Appendix K, s. 44(1.1)]	Disagree.	Page 25
20	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Complaint Investigation Process	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. [Appendix K, s. 44(2) and (4)]	Disagree. The current 10-business-day period for representations is effective in the vast majority of cases and supports the timely resolution of complaints. The Office already has flexibility to accept additional submissions where necessary.	Page 47
21	Complaint Investigation Process	That the Act be amended to: Reduce the commissioner's optional extension to the informal resolution process by five days. [Appendix K, s. 44(5)]	Disagree. Changes to the number of business days are not required. However, OIPC is requesting an amendment in to this provision, to allow for extensions to be at the discretion of the Commissioner.	Page 47
21	Complaint Investigation Process (Suggestion)	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.	Acknowledgment that no legislative changes are required. This suggested approach is consistent with OIPC's current practice.	
21	Complaint Investigation Process (Suggestion)	The OIPC formally advise the complainant and the public body of the cessation of the informal resolution process.	Acknowledgment that no legislative changes are required. This suggested approach is consistent with OIPC's current practice.	Page 47
21	Complaint Investigation Process (Suggestion)	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).	Acknowledgment that no legislative changes are required. This suggestion is not practical or possible in all circumstances. The existing practices of OIPC attempt to provide public bodies with preliminary assessments during the investigation process. OIPC uses best efforts when possible to provide public bodies with reasonable outcome expectations.	Page 47
21	Complaint Investigation Process (Suggestion)	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.	Acknowledgment that no legislative changes are required. The existing practices of OIPC provide public bodies with opportunities to provide additional submissions when circumstances require.	Page 47
21	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Extent of the Appeal Right	That the Act be amended to: Allow a person to file a complaint for failure to comply with a obligation under the Act. [Appendix K, s. 42]	Agree.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
21	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Extent of the Appeal Right	That the Act be amended to: 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". [Appendix K, s. 42(1) and (2)(a), s. 47(e), s. 52(1), (2)(a), and (3), s. 56(4)(b), s. 59(1), s. 83(1)]	Partially Agree; however, unsure if "failure to act" should be deleted.	
22	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Extent of the Appeal Right	That the Act be amended to: 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. [Appendix K, s. 50(1)(c)]	Agree.	
22	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Extent of the Appeal Right	That the Act be amended to: 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. [Appendix K, s. 51(2)(c)]	Agree.	
22	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Extent of the Appeal Right	That the Act be amended to: 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. [Appendix K, s. 54(1) and (2)]	Agree.	
22	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Deemed Acceptance and the Appeal Right	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. [Appendix K, s. 49(3) and (4), s. 54(2)]	Disagree. There is a big difference between acceptance of a recommendation vs. compliance with a recommendation.	
22-23	COMPLAINTS, RECOMMENDATIONS AND APPEALS - The Court Process	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. [Appendix K, s. 57]	Disagree.	
23	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Application to the Supreme Court for a Declaration	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. [Appendix K, s. 50(2), s. 79(1)(a)]	Agree.	
23	COMPLAINTS, RECOMMENDATIONS AND APPEALS - Whistleblower Protection (Suggestion)	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.	All public body employees should be afforded whistleblower protections, whether that be through including them within the definition of "public body" under PIDA through regulation or amendment of the act or by including whistleblower protections directly in ATIPPA, 2015.	
23-24	SCHEDULE A - Energy Corporation Act, SNL 2007 C. E-11.01	That section 5.4 of the Energy Corporation Act be amended to allow the standard ATIPPA request, review, recommendation and declaration/appeal processes. [Appendix K]	Agree. Note that the Act is now the Hydro Corporation Act at section 31.	
24	SCHEDULE A - Energy Corporation Act, SNL 2007 C. E-11.01	That ATIPPA, 2015 be amended to extend the section 9 public interest over ride provision to section 5.4 of the ECA. [Appendix K, s. 9(2.1)]	Agree. Note that the Act is now the Hydro Corporation Act at section 31.	

Page # in "Summary Recommendations"	Category	Orsborn's Recommendation	OIPC's Position	Page # in 2026 OIPC Submission (If Applicable)
24	SCHEDULE A - Energy Corporation Act, SNL 2007 C. E-11.01	That the Energy Corporation Act be amended to limit the application of section 5.4 only to hydrocarbon-related information in Nalcor's custody. (Appendix K)	Agree. Note that the Act is now the Hydro Corporation Act at section 31.	
24	SCHEDULE A - Energy Corporation Act, SNL 2007 C. E-11.01	That government considering 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.	Agree. Note that the Act is now the Hydro Corporation Act at section 31.	
24	SCHEDULE A - Evidence Act, RSNL 1990, c. E-16 and Patient Safety Act, SNL 2017 c. P-3.01	That the Act be amended to remove section 8(1) of the Evidence Act from Schedule A. [Appendix K, Schedule A (f)]	Agree.	
24	SCHEDULE A - Fish Inspection Act, RSNL 1990 c. F-12	That the Act be amended to remove section 5(1) of the Fish Inspection Act from Schedule A. [Appendix K, Schedule A (h)]	Agree.	
24-25	SCHEDULE A - Fisheries Act, SNL 1995, c. F-12.1	That the Act be amended to remove section 4 of the Fisheries Act from Schedule A. [Appendix K, Schedule A (i)]	Agree.	
25	SCHEDULE A - Innovation and Business Investment Corporation Act, DNL 2018 c. 1-7.1	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. [Appendix K]	Agree.	
25	SCHEDULE A - Innovation and Business Investment Corporation Act, DNL 2018 c. 1-7.1	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. [Appendix K]	Agree.	
25	SCHEDULE A - Oil and Gas Corporation Act, SNL 2019 c. O-6.1	That section 23 of the Oil and Gas Corporation Act be amended to allow the standard ATIPPA request, review, recommendation and declaration/appeal processes. [Appendix K]	Agree.	
25	SCHEDULE A - Oil and Gas Corporation Act, SNL 2019 c. O-6.1	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.	Agree.	
25-26	SCHEDULE A - Workplace Health, Safety and Compensation Act, RSNL 1990 c. W-11	That the Act be amended to remove section 18 of the Workplace Health, Safety and Compensation Act from Schedule A. [Appendix K, Schedule A (t)]	Agree. Note that it is now section 19 of the Workplace, Health, Safety and Compensation Act, 2022.	

The Office of the Information and Privacy Commissioner and Solicitor-Client Privilege

Arguably the most important mandate of the OIPC in the access to information context is to fulfil the purpose of the Act as expressed in section 3(2)(f):

3. (1) *The purpose of this Act is to facilitate democracy through*
- (a) ensuring that citizens have the information required to participate meaningfully in the democratic process;*
 - (b) increasing transparency in government and public bodies so that elected officials, officers and employees of public bodies remain accountable; and*
- [...]*
- (2) *The purpose is to be achieved by*
- [...]*
 - (f) providing for an oversight agency that*
 - [...]*
 - (iii) provides independent review of decisions made by public bodies under this Act,*

The NL OIPC has had the unusual experience as an oversight body of having been provided with, stripped of and restored twice, and now being challenged on, the authority, during the investigation of a complaint, to compel the production of records where there has been a denial of access to information on the basis of a claim of solicitor-client privilege.

ATIPPA, as it existed at proclamation in 2005, provided the OIPC statutory authority to compel production and review such records. The first challenge to the OIPC’s authority to compel and review records came in 2009, when the Department of Justice challenged our authority to do so, resulting in a decision in favour of the Department in 2010, *Newfoundland and Labrador (Attorney General) v. Newfoundland and Labrador (Information and Privacy Commissioner)*, 2010 NLTD 31. That decision was overturned by the Court of Appeal in *Newfoundland and Labrador (Information and Privacy Commissioner) v. Newfoundland and Labrador (Attorney General)*, 2011 NLCA 69.

No sooner had the Court of Appeal issued its judgment, the Government of Newfoundland and Labrador, upon completion of the first statutory review of *ATIPPA*, amended the *ATIPPA* to remove the authority and mandate of the Commissioner to review claims of solicitor-client privilege in the course of an access to information review investigation. That amendment was part of Bill 29, which was roundly condemned in the public discourse of the day as having the

effect of impairing the Commissioner's ability to perform his function, because he was unable to independently verify the claims of public bodies when reviewing of their decisions to deny access to information. Under the Bill 29 version of the Act, the only route available for independent review for such denials of access was through the time-consuming, resource-intensive, and costly court process. The removal of the first level of independent review by the Commissioner placed an unnecessary burden upon the Courts and impacted the purposes of the Act, as access delayed is often access denied.

The entire history of this matter, including submissions by the OIPC and others, was thoroughly addressed in the Report of the 2014 Statutory Review of the ATIPPA, beginning at page 109 (section 3.5) of the full Report. All submissions to that review by parties other than the government itself expressed that the Commissioner must have this authority restored:

Most participants who commented on solicitor-client privilege felt that the Commissioner must be able to read all documents, including solicitor-client privileged documents and documents involving Cabinet confidences. They expressed the view that the statutory provision as it existed before Bill 29 should be restored. In discussions with the Committee, participants often argued that the reason the Commissioner should be able to examine documents subject to a claim of solicitor-client privilege is that otherwise the Commissioner will be unable to perform his duties properly. That is also the basis on which Justice Harrington concluded (above) that it was "absolutely necessary" for the Commissioner to be able to compel production of solicitor-client privileged documents.

The 2014 Statutory Review Report thoroughly reviewed the existing case law and the policy rationale for the Commissioner to retain the authority to review claims of solicitor-client privilege when conducting an access to information complaint investigation. The Committee determined that this authority must be restored to the Commissioner, and made the following specific recommendations to that effect:

The Committee recommends that

22. The revised Act contain a provision similar to existing section 21 respecting solicitor-client privilege.

23. The Act have no restriction on the right of the Commissioner to require production of any record for which solicitor-client privilege has been claimed and the Commissioner considers relevant to an investigation of a complaint.

24. The Act provide that the solicitor-client privilege of the record produced to the Commissioner shall not be affected by disclosure to the Commissioner pursuant to the Act.

25. The Act not contain any limitation on the right of a person refused access to a record, on the basis that the record is subject to solicitor-client privilege, to complain to the Commissioner about that refusal.

26. The Act contain a provision that would require the head of a public body, within 10 business days of receipt of a recommendation from the Commissioner that a record in respect of which solicitor-client privilege has been claimed be provided to the requester, to either comply with the recommendation or apply to a judge of the Trial Division of the Supreme Court for a declaration that the public body is not required, by law, to provide the record.

27. The Act contain provisions requiring that the application to the Trial Division for a declaration be heard by use of the most expeditious summary procedures available in the Trial Division.

28. The Act contain provisions prohibiting the imposition, by any public body, of conditions of any kind on access by the Office of the Information and Privacy Commissioner to a requested record for which solicitor-client privilege has been claimed, other than a requirement, where there is a reasonable basis for concern about the security of the record, that the head of the public body may require the Office of the Information and Privacy Commissioner official to attend at a site determined by the head of the public body to view the record.

29. The Act contain a provision that prohibits disclosure by the head of a public body of information that is subject to solicitor-client privilege of a person that is not a public body.

The above recommendations were accepted by government, and in fact the House of Assembly voted unanimously to accept (with two minor, unrelated amendments) the draft Bill developed by the Committee, which included specific language intended to fulfil those recommendations. After the coming into force of the *ATIPPA, 2015* the OIPC resumed its former practice of reviewing claims of solicitor-client privilege, which often, but not always, involved obtaining a copy of the records for that purpose from the public body. After the review is over, all records obtained from a public body are subject to the OIPC's records destruction protocol that is strictly observed.

This process continued without incident until 2019, when a complaint was received by the OIPC in relation to a decision by the Department of Justice and Public Safety (JPS) to refuse access to records on the basis of a claim of solicitor-client privilege. During the course of our investigation, JPS refused to provide a copy of the responsive records for our review, and indeed refused to provide any evidence that the records are subject to solicitor-client privilege. Having failed to discharge its burden of proof, the Commissioner was reluctantly left with no choice but to recommend, in [Report A-2019-019](#), that the information be disclosed. JPS then proceeded to seek a declaration under section 50 that it need not comply with the Commissioner's recommendations. No date for that hearing has yet been set at the time of writing.

JPS indicated that its new position on the Commissioner's authority to compel production of and review claims of solicitor-client privilege resulted from the issuance of a decision by the Supreme Court of Canada in [Alberta \(Information and Privacy Commissioner\) v. University of](#)

[Calgary 2016 SCC 53](#). JPS appears to have waited for two years after that ruling for the right opportunity to take this position. While we appreciate that governments must ensure that its statutes are not in conflict with Supreme Court of Canada rulings, the course of action taken by JPS, particularly given the history of this issue in this province, is puzzling. Our view is that the statutory language in *ATIPPA, 2015* clearly gives the OIPC the authority to review claims of solicitor-client privilege. Their position is that it does not.

From a broader perspective, the Legislature made an unequivocally clear policy choice to follow the unambiguous direction provided by the Report of the 2014 Statutory Review. In fact, then-Minister Steve Kent, responsible for *ATIPPA* at the time, explicitly said so, as recorded in Hansard when speaking on the Bill on April 23, 2015:

Now, Mr. Speaker, I would like to touch on the role of the Office of the Information and Privacy Commissioner. The Commissioner plays a fundamental role in the administration of the Access to Information and Protection of Privacy Act. This bill strengthens the role of the Office of the Information and Privacy Commissioner as an advocate for access to information and protection of personal information. Specifically, the bill increases the powers of the Information and Privacy Commissioner to include responsibility for approving extensions of time for ATIPP requests and the power to review various types of records including Cabinet records, solicitor-client privilege records, and other records in the custody or under the control of the public body. [emphasis added]

The specific provisions that were added under *ATIPPA, 2015* occurred prior to the University of Calgary court decision. In that decision, the Court found that language in Alberta's *Freedom of Information and Protection of Privacy Act* which the Commissioner in that Province relied on as giving it the authority and mandate to review claims of solicitor-client privilege was not sufficiently clear enough because it did not explicitly refer to solicitor-client privilege. The phrase in question, from section 56(3) of Alberta's Act, is "despite any privilege of the law of evidence," which is similar to section 97(1)(d) of *ATIPPA, 2015*: "This section and section 98 apply to a record notwithstanding (d) a privilege under the law of evidence."

Although the 2014 Statutory Review Committee did not have the advantage of having the University of Calgary decision available to them, they were well aware that solicitor-client privilege cannot be abrogated without clear and explicit statutory language. For that reason, the Committee included the following provisions in its draft statute, which were accepted by the Legislature without alteration, and form part of the *ATIPPA, 2015* as follows:

97(5) The head of a public body may require the commissioner to examine the original record at a site determined by the head where

(a) the head of the public body has a reasonable basis for concern about the security of a record that is subject to solicitor and client privilege or litigation privilege;

(6) The head of a public body shall not place a condition on the ability of the commissioner to access or examine a record required under this section, other than that provided in subsection (5).

100 (2) The solicitor and client privilege or litigation privilege of the records shall not be affected by production to the commissioner.

Clearly, the 2014 Statutory Review Committee recognized that the phrase “notwithstanding a privilege under the law of evidence” was, by itself, perhaps not sufficient to fully nail the door shut and unquestionably establish the Commissioner’s authority to review claims of solicitor-client privilege, and by extension, so did the Legislature. On that basis, the additional provisions cited above were introduced to make it explicitly clear. Unfortunately for Alberta’s Commissioner, none of these additional provisions are present in Alberta’s Act, and as a result, we have the University of Calgary decision from the Supreme Court of Canada.

In the context of the lengthy analysis of issues by the Statutory Review Committee, the specific recommendations in its Report, and the statutory provisions in the *ATIPPA, 2015*, it is difficult to see how anyone can look at that evidence and not see that the Committee went to great lengths to remove any possibility of doubt that the Commissioner is intended to be able to compel the production of and conduct a review of records where there has been a claim of solicitor-client privilege in the context of an investigation by the Commissioner into a decision to refuse access to an access to information requester.

During the debate on Bill 29, current Attorney General Andrew Parsons fought against any restriction on the Commissioner’s ability to review claims of solicitor-client privilege, as recorded in Hansard on June 11, 2012:

Mr. Speaker, government is introducing a blanket exemption on the release of any information touching upon solicitor-client privilege; any appeal must be done through the Supreme Court rather than through the Privacy Commissioner.

Mr. Speaker, why is government forcing people of this Province into expensive and lengthy legal court action on matters which could easily be avoided by referring to the Privacy Commissioner?

[...]

I referred earlier, Mr. Speaker, to a Supreme Court, Court of Appeal decision. It was a case between the Information and Privacy Commissioner. This was an appeal of a decision at the Trial Division level. It was between the Privacy Commissioner and the Attorney General of Newfoundland and Labrador. In this case, which is quite a substantial decision, an individual in the Department of Justice requested their own file. What happened here is the department said: No, you cannot see your own file. We are not letting you have it. It is all privileged. This person had to go to court. It is funny when you read some of the comments made by the judges in this case.

One of the things that struck me when I looked at it was some of this stuff that makes up part of a person's record might be things like pay stubs and employment

information. Sure, it could even be a resume or the resume submitted when they got the job. Who knows what is in the person's employment file? In this case, instead of going through it and actually making it look like they looked through the file and could pass back some stuff, what they did was a blanket coverage of: you are not going to get it; you are not going to see this.

That was one of the concerns expressed in the decision. This was done with a majority; you had the three Supreme Court judges agreeing on this. One of the things they discussed, Mr. Speaker – and this is what they call obiter. It is just reasons that were brought up here. "The court is concerned by the possibility of misuse of authority conferred by the legislation." That is what we are doing now; we are getting around this court's decision. We are getting around the concerns expressed by this court because we are going to change the legislation. We are going to allow this blanket coverage. We are going to allow government to wipe away people's rights to access the information.

Really, if you think about it, it is an iron curtain government that we are moving into here. We are moving into a – I have heard these terms out there, repressive, secretive, draconian, regressive, these all apply. You can check off all these boxes, Mr. Speaker, because they all apply in this case.

One of the forms of misuse would be for the Department of Justice to claim a blanket privilege for files. That is one of the things – and I know it is hard work. I know it takes time to go through people's files to see what is privileged and what is not privileged, I understand that. The fact is that not everything is privileged, not everything. There are things in there that have nothing to do with any form of privilege. In this case what we are getting at was there is an attempt, Mr. Speaker, to cover everything, to just say no, we are not going to do that. That is what you see as time goes on.

With ATIPPA, 2015, a clear policy choice was made by the Legislature after a thorough analysis of the issues canvassed by the 2014 Statutory Review Committee, and explicitly stated as such by the Minister when introducing the new Act in the Legislature. Even if the present government legitimately harbours some doubt, in light of the University of Calgary decision, whether the statutory language in ATIPPA, 2015 is entirely sufficient for its intended purpose, there were two choices before it. It could have introduced an amendment in the legislature to add additional language for greater certainty. For reasons unknown to the OIPC, it chose instead to simply refuse to provide records to the Commissioner for review where there was a claim of solicitor-client privilege. In doing so, it opened up another era of uncertainty, whereby some public bodies are following suit and others not, creating an unnecessary standoff which will see matters continue to clog up the court system, for the benefit of whom? This has been a baffling and frustrating experience for the OIPC as well as access to information requesters who must now wait an indefinite period of time for their matters to be resolved. In terms of the effect on requesters, our [Report A-2013-004](#), particularly paragraphs 36 through 40, illustrates the path that these matters can take when there is no opportunity for review by the Commissioner.

It is the view of the OIPC that the statutory language in *ATIPPA, 2015* is more than sufficient to ensure the Commissioner's authority to compel the production of and review records where there has been a complaint about a refusal of access on the basis of a claim of solicitor-client privilege. In light of the current circumstances, however, we believe it would be advisable to bring this saga to a final conclusion through a further legislative amendment, similar to that which was made by the federal government following the University of Calgary decision. The federal *Access to Information Act* contained language similar to that found in Alberta's *Freedom of Information and Protection of Privacy Act*, but lacked the additional provisions noted above that were added in *ATIPPA, 2015*. The federal *Access to Information Act* was therefore amended. The original version of the federal Commissioner's authority is as follows:

36(2) Notwithstanding any other Act of Parliament or any privilege under the law of evidence, the Information Commissioner may, during the investigation of any complaint under this Act, examine any record to which this Act applies that is under the control of a government institution, and no such record may be withheld from the Commissioner on any grounds.

Prior to the 2019 amendments, section 36(2) was the only authority in the federal statute upon which the Commissioner could ground his or her authority to examine records, including records where there was a claim of solicitor-client privilege. Section 36 has since been replaced and states:

36 (2.1) The Information Commissioner may examine a record that contains information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege only if the head of a government institution refuses to disclose the record under section 23.

(2.2) For greater certainty, the disclosure by the head of a government institution to the Information Commissioner of a record that contains information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege does not constitute a waiver of those privileges or that professional secrecy.

As with the pre-2019 federal legislation, Alberta's statutory provision that was at issue in the University of Calgary case did not specifically include the phrase "solicitor-client privilege". The language in section 97 of *ATIPPA 2015*, however, explicitly uses the phrase "solicitor client privilege or litigation privilege" and clearly authorizes production of records to the Commissioner for review. In addition, the legislation in Alberta had no safeguards in place to protect the privilege upon production to the Commissioner. Sections 97(5)(a) and 100(2) explicitly protect the privilege in this Province.

Our recommendation to the Chair of this Review is that an amendment to the *ATIPPA, 2015* is required, not because the current statutory language is insufficient, but simply to bring an end to what has been a seemingly endless campaign, irrespective of political stripe, of governments of this Province wishing to impair the ability of the Commissioner to discharge his role as derived from the purpose of the *ATIPPA, 2015*. Such an amendment would re-

affirm, once and for all, the policy choice that was adopted by the Legislature in 2015, and supported by the current Attorney General by his vote in favour of the new statute, as well as in debate over Bill 29 in 2012. The current legislation contains the necessary safeguards to protect solicitor-client privilege upon disclosure to the Commissioner, and public bodies always have the right to ask the Court to review the matter following an assessment by the Commissioner. The challenge to this first level of independent review is unnecessary and contrary to meaningful access to information.

Recommendation 1.1: Amend section 97(1) by adding after (d) a specific provision with effect similar to section 36(2.1) of the federal *Access to Information Act*.

Access to Information Complaints and Appeals

Some issues with this part of *ATIPPA, 2015* have impacted clarity and user-friendliness, which could be addressed through targeted amendments.

Applicant’s Path to Appeal Following Commissioner’s Recommendation under 47(b)

Section 47(b) sets out an option for the Commissioner to recommend that a public body reconsider its decision to refuse access to a record or part of a record. Such an option is well-suited to a scenario where the public body has applied an exception, and the OIPC has received a complaint and agrees that the exception applies, but it is clear that the public body has not adequately considered the exercise of discretion. While these scenarios are not frequent, they do occur, and we believe a provision like section 47(b) has a place in *ATIPPA, 2015*.

The circumstance here is not one in which there is a public interest to the extent that section 9(1) comes into play. In weighing the purpose for the exception against the reasons for exercise of discretion, there are times when public bodies have failed to fully take into account those impacts in comparison with the reason for the exception, and have withheld information when disclosure would cause little if any harm.

Despite the intent of section 47(b), we have not utilized it in any Commissioner’s Reports. The main reason for this is uncertainty regarding the appeal process. In the circumstance described above, we could issue a Report making a finding that the exception applies and a recommendation under 47(a) that the public body refuse access, and this clearly preserves the applicant’s right to file an appeal in section 54. While we believe that a recommendation under section 47(b) would result in either a new or a re-confirmed decision, it is not clear where that leaves the applicant’s right to appeal. Arguably the new or reconfirmed decision could then come back to the Commissioner for review, however if we have already agreed that the exception applies, it is not clear what the process is from there to an appeal.

Recommendation 13.1: Amend Part II, Division 3 to clarify that the applicant retains a path to appeal in the Trial Division if the Commissioner makes a recommendation under 47(b).

Clarity of Breadth of Applicant’s Right of Appeal

It is our view that any time an access to information applicant files a complaint under section 42, there is a clear path through the Commissioner’s review process to an appeal at the Trial Division. Section 42 is quite broad in its language – the threshold is that the complaint must be a matter “respecting a decision, act or failure to act of the head of the public body” and it need only “relate to the request” for access or correction. Under *ATIPPA, 2015*, a complainant

has two options – they may go to the OIPC, or they may go directly to the Trial Division, where the language in section 52(1) closely mirrors that of section 42.

A decision, act, or failure to act takes in a lot of ground. Particularly when it comes to a failure to act, some of those alleged failures can relate to a failure to assist the applicant in making the request. Section 13 of *ATIPPA, 2015* requires that public bodies respond without delay in an open, accurate and complete manner. The duty to assist in section 13 is a common feature of access to information statutes everywhere, and numerous Commissioner's Reports have been issued dealing with that subject, including, for example, the duty to conduct an adequate search for records. The standard for an adequate search, in brief, is that public body officials who are knowledgeable about the subject matter of the request must search where such records are reasonably likely to be found. Often adequacy of search issues are resolved during informal resolution, but not always. If, at the end of the process, the requester has the basis to make a complaint that the search was not adequate, they have an opportunity to make that case directly to the Trial Division in section 52, or to first go to the Commissioner under section 42, which will cost less, occur more quickly, and more often than not will be resolved informally.

If a requester decides to first pursue the matter through a complaint to the Commissioner, they should not be penalized by the placement of a roadblock against subsequent appeal to the Trial Division. In our view, that is not what is intended by the language in section 54(a). Section 54 provides for appeals to court following a public body's response to a Commissioner's Report. Section 54(b) states that an applicant (or third party) may commence an appeal of "the head's decision to grant or refuse access to the record or part of the record." In our view, if a public body decision, act or failure to act results in the applicant not getting the records requested, this amounts to a refusal to grant access, and is encompassed within section 54.

In recent years Memorial University, one of the province's largest and most influential public bodies, has adopted a restrictive view of this process. For example, in issuing our [Report A-2019-032](#) we agreed that Memorial had conducted a reasonable search, and recommended that it maintain its position regarding the request for records by the Applicant. When we address a reasonableness of search issue, Memorial University has unfortunately developed boilerplate language which it inserts in its section 49 letter of response that states:

Subsection 49(3) of the ATIPPA, 2015 requires us to give notice of the right to appeal where it exists but, in this case, we do not believe s. 54 grants a right of appeal because the recommendation is not to grant "access to the record or part of the record" or "make the requested correction of personal information."

In our view, this is contrary to section 49, which requires the head of the public body to decide whether to follow our recommendations (49(1)(a)) and give written notice of that decision to relevant parties. Section 49(3) specifies the contents of that notice, including the right of appeal. In our view, such an approach to statutory interpretation is not consistent with the purpose of *ATIPPA, 2015* and contrary to the principles of statutory interpretation. Eventually

this may have to be addressed by a Court, however this statutory review presents an opportunity to do so that will avoid the cost and delay of a court process for all parties.

Recommendation 13.2: Amend Part 2, Divisions 3 and 4 for greater certainty to clearly establish that an applicant's right of appeal to the Trial Division following a complaint to the Commissioner's Office is equally as broad as the right of appeal granted under section 52 when the applicant goes directly to court, and that it encompasses any decision, act or failure to act which results in the applicant not receiving the requested records.

Disposition of an Appeal

As a further issue, despite the language in sections 42 and 52 that allow a complaint or appeal for any "decision, act or failure to act of the head of the public body that relates to the request," the language in section 60 regarding disposition of an appeal is narrower. If the matter in question is an alleged failure on the part of the public body to conduct an adequate search, in our view this is clearly an allegation of a failure to act. However, the language in 60(1)(c)(ii) that would allow the Court to make an order the court considers appropriate is tied to a scenario in 60(1)(c) where the Court has determined that the head is not authorized or required to refuse access to records. In reality, if an adequate search has not been conducted and there may be further responsive records that have not been found, it will not be possible for the Court to rule on those records. While an argument could be made that the Court can exercise its inherent jurisdiction, or that it could conduct an interpretive exercise in light of sections 42 and 52 and the purpose of the Act to find that it has the authority to make an order regarding the search, it is equally possible that a Court will find that it has no authority beyond what is provided in section 60 to dispose of an appeal. Although not reflected in any written judgments, the limitations of section 60 have been the cause of some discussion among parties and the Judge in the courtroom. In this absurd result, a public body could, either through incompetence or bad faith, fail to conduct an adequate search for records and its response would simply be to indicate that there are no responsive records. The *ATIPPA, 2015* must clearly provide a means to rectify such a circumstance, otherwise there is a risk that the right of access around which the Act is based could be frustrated.

Recommendation 13.3: Amend section 60 allowing the court to make an order that it considers appropriate, and have that provision stand alone as 60(1)(d).

Ex Parte Applications for a Declaration under Sections 50 and 79

When a public body applies under section 50 (or 79) to the Trial Division for a declaration that the public body is not required to comply with a recommendation of the Commissioner, section 50(3) requires the head to serve a copy of the application on the Minister responsible for the Act, the Commissioner, and a person who was sent a copy of the report. Section 50(4) gives those parties an opportunity to become intervenors in that application.

There is no indication in *ATIPPA, 2015* that the Commissioner is intended to be the respondent for this declaration application. The fact that the Commissioner is given equal standing to intervene, along with the Minister and a person who was sent a copy of the report, indicates that status. The public body's declaration application is clearly an *ex parte* application, and the Commissioner has the option not to be a party to the application. Unfortunately, it has commonly been assumed that the Commissioner is the respondent, and public bodies have constructed their applications based on this assumption. Some language in section 50 (and 79) to indicate that the application for a declaration is an *ex parte* application would be helpful.

Recommendation 13.4: Amend *ATIPPA, 2015* to clarify that an application by a public body for a declaration under sections 50 and 79 is an *ex parte* application.

Public Body Notification of Applicant on Third Party Appeal

Section 56(3) says that the Minister responsible for the *Act*, the Commissioner, the applicant or a third party may intervene in an appeal. Section 56(2) contains a requirement for the appellant to service notice of the appeal on the Commissioner and the Minister responsible for the *Act*. If the appellant is the third party, the third party would not normally know the identity of the access to information applicant. While section 15(1)(b) requires the public body to advise the applicant of the status of the request, we have found that public bodies have not understood this to mean communication about the status of a matter that has proceeded to an appeal.

Recommendation 13.5: Amend section 56 of *ATIPPA, 2015* to require a public body to provide a copy of an appeal received from a third party to the access to information applicant and inform them of their right to intervene under section 56(3).

We have observed, on several occasions, some of which are ongoing, situations where a third party appeal is under way at Court but it is unclear if the access to information requester continues to be interested in receiving the contested records. We have seen scenarios where the email and/or mailing address / telephone number of the requester is either no longer valid, or no responses are received when attempts have been made to reach the requester. This issue is usually only discovered some time into the appeal process. Usually applicants are quite interested in the outcome and are patiently awaiting the result of the third party appeal. In one specific case the access request was made on a client's behalf by a lawyer who later left the law profession. Multiple attempts have been made to determine the identity of the Applicant to no avail.

The Applicant is not required to participate in a third party appeal, as the third party bears the burden of proof. The Applicant, therefore, should not be punished for remaining silent and awaiting the outcome. On the other hand, there is a cost to the parties involved to proceed with a review of a third party's appeal when the matter may be moot, if the Applicant is no

longer interested in obtaining the records. From the third party's perspective, although it might appear that the Applicant is no longer interested, if the third party withdraws their appeal, that means disclosure of the information is no longer contested, and the public body is obligated to send the information to whatever address for the Applicant is on file. In cases where the email/ mailing address/ phone number are no longer valid, the risk for the third party may be low; however, in cases where the Applicant has simply chosen to remain silent, third parties are understandably reluctant to simply withdraw.

Recommendation 13.6: Amend Part II, Division 4 to provide that a party to an appeal can make an interlocutory application to seek a ruling that an access to information request can be deemed abandoned if it is not possible to ascertain whether the access to information applicant remains interested in receiving the requested records and all reasonable efforts have been made by the public body to confirm the applicant's continued interest in the outcome.

Artificial Intelligence

Artificial Intelligence, or AI, is a term used to describe an evolving approach to technological solutions which includes the use of automated decision-making processes. Businesses and governments around the world have begun to use AI in their decision-making processes, including examples such as [medical treatments](#), [applications for government aid](#), or even [sentencing in criminal cases](#). It has also been the subject of a great deal of scrutiny in the academic world. For example, in September 2020 the Citizen Lab at the University of Toronto published a report containing a critical analysis of the use of AI in law enforcement, entitled: [To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada](#).

We do not know at present whether a public body in this province has or intends to implement AI, or if any such plans are on the drawing board. What we do know is that our privacy oversight counterparts across Canada and around the world are beginning to see such initiatives and are paying close attention. The Global Privacy Assembly, representing membership of privacy oversight bodies around the world, passed a unanimous [resolution](#) on Accountability in the Development and Use of Artificial Intelligence during its annual conference (held online) in October 2020. The entire resolution is captured in Appendix F, however part 4 of the resolution specifically refers to the need to create a statutory regime to protect privacy and human rights in the development of AI:

4. Encourage governments to consider the need to make legislative changes in personal data protection laws, to make clear the legal obligations regarding accountability in the development and use of AI, where such provisions are not already in place

Canada’s federal Office of the Privacy Commissioner (OPC) initiated a broad [consultation](#) process on the subject in early 2020, and on November 12 released its [recommendations](#) for a regulatory framework for Artificial Intelligence to be implemented as reform of the [Personal Information Protection and Electronic Documents Act](#) (PIPEDA) which covers private sector organizations.

One of the challenges of AI is that while its implications encompass privacy issues, those implications are also much broader than privacy, and in fact part of the premise of AI is diametrically opposed to one of the foundational principles of privacy. For example, the principle of data minimization, which has long been entrenched in privacy laws, means that entities should only collect, use, and disclose the minimum amount of personal information necessary for the intended purpose. AI, however, generally works on the premise that it has a massive amount of data to work with in order to discern patterns and, through automated decision-making, make choices based on that data. In theory, the more data, the better the decision.

If we were to adopt an approach purely from a privacy perspective, AI would be a non-starter based on data minimization alone. We do, however, recognize that AI promises not only risks,

but great benefits to society. On that basis, privacy and AI experts the world over are attempting to develop a framework that works for both.

In April 2019 the Government of Canada implemented a new [Directive on Automated Decision-Making](#). The Directive sets out minimum requirements for federal government departments that wish to use an Automated Decision System – essentially technology that either assists or replaces the judgement of human decision-makers. Among other things, the Directive requires that an Algorithmic Impact Assessment be conducted prior to the implementation of any automated decision-making process. The objective is to ensure that such technology is deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent and interpretable decisions. The directive is intended to achieve the following results:

Decisions made by federal government departments are data-driven, responsible, and comply with procedural fairness and due process requirements.

Impacts of algorithms on administrative decisions are assessed and negative outcomes are reduced, when encountered.

Data and information on the use of Automated Decision Systems in federal institutions are made available to the public, where appropriate.

The Government of Canada has also proposed the idea of creating a Data Commissioner. Although the scope of that role has not been determined, it could potentially serve a function adjacent to the Federal Privacy Commissioner, but beyond privacy, and it could oversee broader implications for the use of data, such as those implications intended to be assessed by an Algorithmic Impact Assessment.

Realistically, in Newfoundland and Labrador, we are unlikely to see the creation of a separate Data Commissioner in the foreseeable future. We are, however, likely to see AI and automated decision-making at some point, and perhaps sooner rather than later, in light of the rate of expansion of this technology around the world. In a small jurisdiction, one often needs to wear several hats. While AI creates substantial challenges for effective oversight of legal and ethical implications, there is already a substantial overlap with privacy oversight that positions the OIPC well to take on that role. Some of the challenges inherent in attempting to apply a traditional privacy lens to AI, without alteration or augmentation, was captured recently by Ontario's Information and Privacy Commissioner in her [comments](#) on the creation of a new privacy statute in that province:

While Purpose Specification, Consent, and Collection Limitation continue to be relevant principles, a more modern private sector privacy law would need to reconsider the weight ascribed to them relative to other principles in certain circumstances. For example, in an era of artificial intelligence and advanced data analytics, organizations must rely on enormous volumes of data, which runs directly counter to collection limitation. Data are obtained, observed, inferred, and/or created from many sources other than the individual, rendering individual consent less practicable than it once was. The very object of these advanced data processes is to discover the unknown, identify patterns and derive insights that cannot be

anticipated, let alone described at the outset, making highly detailed purpose specification virtually impossible.

It will likely be necessary, as AI matures, for each jurisdiction to develop purpose-built legislation around AI, however we believe it is advisable to start now with some very basic legislative provisions so that the first AI in use by a public body can be required to consider and mitigate any potentially negative implications of such a program, and also to be subject to independent scrutiny. At the same time, some basic oversight functions in *ATIPPA, 2015* could ensure that there is some level of independent scrutiny available and potentially required before AI initiatives become a reality here.

Some collections, uses or disclosures in an AI system, would, as noted above, conflict with current privacy laws. In order to implement an AI program in such a way that they would not be contrary to *ATIPPA, 2015*, in the absence of a comprehensive legislative scheme that incorporates privacy protection while facilitating the development of AI (which as far as we know does not exist anywhere) it is likely that legislation would have to be created specifically for the purpose of facilitating individual AI applications. If this were to occur, the OIPC would be consulted in accordance with section 112. It is unusual for us to receive a draft bill earlier than a week prior to it being tabled in the House, so while we find that process useful and we have been able to effect significant privacy-protective changes in legislation even at that late stage, if government has substantially invested in planning a program that a new bill will be the last step in implementing, it is not likely to be a sufficient process in terms of meaningful engagement and oversight. Furthermore, prior to oversight, it is much more important that clear guardrails are put in place before major political and financial investments in AI are committed.

For those reasons, and in light of the issues described above, it is recommended that *ATIPPA, 2015* be amended to do the following:

Recommendation 7.1: Incorporate a definition of artificial intelligence into *ATIPPA, 2015*.

Recommendation 7.2: Require algorithmic assessments to be conducted by any public body prior to implementation of a program involving the use of artificial intelligence.

Recommendation 7.3: Require a public body intending to develop and implement a program involving the use of artificial intelligence to notify the Commissioner of that intention and engage the Commissioner at an early stage of the development of that program, including providing to the Commissioner a copy of an algorithmic assessment for review and comment by the Commissioner prior to implementation of the program.

Recommendation 7.4: In addition to privacy and access to information issues, in its review and assessment, the OIPC should be entitled to comment on all

implications for the use of AI in the proposed program, including data ethics factors such as proportionality, fairness and equity, in a manner comparable to a Data Commissioner; to this end, amendments to the purpose of the *ATIPPA, 2015* would be required to reflect the added mandate for an independent oversight agency that is empowered to review and comment on the implications, including privacy and data ethics implications, for the implementation of artificial intelligence in public body programs. Comparable powers or duties would need to be added to section 95.

These recommendations are compatible with, but less detailed than, those proposed by the federal Office of the Privacy Commissioner, as referenced above, that if implemented would cover the private sector alongside *ATIPPA, 2015* coverage of the provincial public sector. In particular, the recommendation to require that public bodies complete an Algorithmic Impact Assessment for AI applications, with mandatory review by the OIPC, is consistent. As noted above, however, we do not at this time make detailed recommendations for a comprehensive regulatory regime including such things as a right to meaningful explanation (the right of an individual to know how an AI made a decision) and a right to contest (the right to appeal such a decision). While these are important principles, our perspective at this time is that without examples of AI to inform us, developing a regime would be premature and speculative. We anticipate that the proposed Algorithmic Impact Assessment and review process, alongside our existing authorities to conduct complaint-based and own-motion investigations related to privacy, will provide sufficient safeguards at this stage.

This said, the OPC does make important recommendations about demonstrable accountability and traceability that deserve attention and relate to our Recommendation 3.1 about Duty to Document. We recommend on this subject that a legislative duty to document be created, with OIPC oversight, and that it be high-level and principle-based, with implementation at the public body level to be policy-based but appropriate for its operations and context. As it relates to AI, the key is to require a granular level of documentation of processing to ensure that, if a public body's decision has been automated, then there is an ability to understand and potentially contest that decision. The OPC cites [Article 30 of the European Union's General Data Protection Regulation](#) as an example of a legislative model addressing this topic. Quebec's [Bill 64](#) (section 102) is a new Canadian example of a statute that contains provisions that address a number of the topics referenced, including record keeping but also the right to an explanation and the right to contest. [Bill C-11](#) at section 63(3) also contains a transparency requirement for automated decision-making, with "automated decision system" being a defined term in the Bill.

Recommendation 7.5: Introduce a special Duty to Document requirement for Artificial Intelligence applications that requires that records of processing activities be maintained.

Indigenous Issues

Does ATIPPA, 2015 sufficiently recognize and address privacy and access to information issues relating to Indigenous communities? We have not been presented with many specific issues that would raise this question, however there may be issues that have not come to our attention. We did, however, recently issue [Report A-2020-020](#) regarding a request for access to information to the Intergovernmental and Indigenous Affairs Secretariat, which is now the subject of an application for a declaration under section 50. In light of the increasing awareness of concerns regarding Indigenous peoples in Canada, the time may be right during this legislative review to consider this question.

We conducted a jurisdictional scan to examine whether, and the extent to which, comparable statutes reference indigenous communities. The results are available at Appendix G.

Currently, *ATIPPA, 2015* references the Nunatsiavut Government in the intergovernmental relations provision at section 34. It may be appropriate for the Chair to consider whether other types of indigenous entities should be referenced in *ATIPPA, 2015*, and if so in what way? Are there special access to information and protection of privacy issues in indigenous communities that deserve attention, and if so, should those concerns be addressed in *ATIPPA, 2015*, or should they be addressed within the legal frameworks of those particular communities?

The Chair may need to consider the extent to which these questions are within the mandate of this legislative review, but to the extent that they may be, consultation with affected communities would be a necessary first step. We include the appended results from our jurisdictional scan as additional context.

Recommendation 11.1: Initiate consultation with Indigenous organizations and governments in Newfoundland and Labrador, among other stakeholders such as the Intergovernmental and Indigenous Affairs Secretariat, to consider whether and how Indigenous organizations and governments could be referenced in the statute.

Appendix F – List of Recommendations

The following recommendations include those arising from the 2026 submissions, together with recommendations carried forward from the 2020 submissions. All recommendations contained in this submission reflect the OIPC's current position. Recommendations carried forward from the OIPC's 2020 submission have been reproduced and retain their original numbering, with the addition of the year identifier "2020".

Review of 2020 Recommendations

2026-1: See [Appendix A](#) for OIPC's position regarding the 2020 Statutory Review Recommendations.

Solicitor-Client Privilege

2026-2: Amend section 97(1) by adding after (d) a specific provision with effect similar to section 36(2.1) of the federal **Access to Information Act**.

Settlement Privilege

2026-3: No amendment of ATIPPA, 2015 to insert a settlement privilege exception.

Workplace Investigations

2026-4-1: Clarify the paramountcy of section 33 with amendments:

- indicating that certain other exceptions in the Act are to be applied to the records before any disclosure, regardless of section 33; and
- ensuring that the exceptions to be applied are subject to a consideration of whether the public interest favours disclosure.

2026-4-2: Amend section 33 to limit disclosure of records relating to a workplace investigation such that the right of access would commence after a workplace investigation has been completed. For clarity, disciplinary decisions need not be finalized or imposed for the right of access to commence and the right of access would be enduring thereafter.

2026-4-3: Consult with public bodies on whether section 33 should be broadened to apply to harassment investigations beyond the employment context.

Third Party Business Interests

2026-5-1: No amendment to the operation of sections 19 and 39 and maintain these sections as they are.

2026-5-2: Amend the Act to provide a 20-year sunset clause on third party business information.

2026-5-3: 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.

2026-5-4: Amend the Act to make the exception for disclosure harmful to third parties' business interests subject to the public interest override.

[Public Interest Override](#)

2026-6-1: Clarify that the burden of proof in the application of the public interest override does not rest solely on the applicant or the public body but that any party, including OIPC at the review stage, is obligated to bring forward evidence that could be relevant to this determination.

2026-6-2: Include third party business information (section 39) among the list of exceptions to access to which the public interest override in section 9(1) applies.

2026-6-3: Consider amending section 9(3) to remove the potential for limitation of its applicability to matters that are "urgent" as a temporal consideration.

[Information Technology Security](#)

2026-7: Replace section 31(1)(l) of ATIPPA, 2015 with British Columbia's security provision at section 15(1)(l) of FIPPA.

[Access Request Timelines and Extensions](#)

2026-8: Maintain the current access to information timelines in section 16 and 23.

[Overdemand by Applicants and Disregard](#)

2026-9-1: Amend section 21(1) to increase the timeline for an application to the Commissioner for approval to disregard an access request from 5 to 10 business days.

2026-9-2: Amend ATIPPA, 2015 to provide authority for public bodies to hold in abeyance access requests over a certain number from the same applicant.

[Informal Resolution Procedure](#)

2026-10: Amend the informal resolution extension provision to be at the discretion of the Commissioner.

[Access to Information Complaints and Appeals](#)

2020.13.1: Amend Part II, Division 3 to clarify that the applicant retains a path to appeal in the Trial Division if the Commissioner makes a recommendation under 47(b).

2020.13.2: Amend Part 2, Divisions 3 and 4 for greater certainty to clearly establish that an applicant's right of appeal to the Trial Division following a complaint to the Commissioner's Office is equally as broad as the right of appeal granted under section 52 when the applicant goes directly to court, and that it encompasses any decision, act or failure to act which results in the applicant not receiving the requested records.

2020.13.3: Amend section 60 allowing the court to make an order that it considers appropriate, and have that provision stand alone as 60(1)(d).

2020.13.4: Amend *ATIPPA, 2015* to clarify that an application by a public body for a declaration under sections 50 and 79 is an *ex parte* application.

2020.13.5: Amend section 56 of *ATIPPA, 2015* to require a public body to provide a copy of an appeal received from a third party to the access to information applicant and inform them of their right to intervene under section 56(3).

2020.13.6: Amend Part II, Division 4 to provide that a party to an appeal can make an interlocutory application to seek a ruling that an access to information request can be deemed abandoned if it is not possible to ascertain whether the access to information applicant remains interested in receiving the requested records and all reasonable efforts have been made by the public body to confirm the applicant's continued interest in the outcome.

Commissioner Vacancy

2026-11: Amend *ATIPPA, 2015* to ensure that there is a designation of an office staff member to act in the role of Commissioner during any period where there is no acting commissioner or commissioner.

Artificial Intelligence

2026-12-1: Incorporate a definition of artificial intelligence into *ATIPPA, 2015*.

2026-12-2: Require algorithmic assessments to be conducted by any public body prior to implementation of a program involving the use of artificial intelligence.

2026-12-3: Create a statutory requirement for a published registry of AI impact assessments, and a corresponding authority for the Commissioner to require that a public body provide a particular AI impact assessment for review upon request

2026-12-4: In addition to privacy and access to information issues, in its review and assessment, OIPC should be entitled to comment on all implications for the use of AI in the proposed program, including data ethics factors such as proportionality, fairness and equity, in a manner comparable to a Data Commissioner; to this end, amendments to the purpose of *ATIPPA, 2015* would be required to reflect the added mandate for an independent oversight agency that is empowered to review and comment on the implications, including privacy and data ethics implications, for the implementation of artificial intelligence in public body programs. Comparable powers or duties would need to be added to section 95.

2026-12-5: Introduce a special Duty to Document requirement for artificial intelligence applications that requires that records of processing activities be maintained.

Biometric Data

2026-13-1: Amend section 2(u)(v) to expressly recognize biometric information within the definition of personal information:

- "(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics."

2026-13-2: Include a definition of "biometric information" as:

- "Information derived from an individual's unique measurable characteristics."
- This definition is consistent with the approaches adopted in Prince Edward Island and Alberta.

2026-13-3: That a Privacy Impact Assessment be mandatory for any program, initiative, or substantial modification involving the collection, use, or disclosure of biometric information.

2026-13-4: That public bodies be required to notify OIPC before implementing any program involving the creation of a biometric database and provide the completed Privacy Impact Assessment to the Office for review and comment before deployment.

2026-13-5: That legislation provides for independent oversight, investigations, complaint resolution, and enforcement mechanisms to ensure accountability and maintain public trust in the use of biometric technologies.

Surveillance Technologies

2026-14-1: Require all organizations to conduct a privacy impact assessment prior to using video surveillance.

2026-14-2: Require all organizations who use video surveillance to have a privacy management program and policies in place that ensure compliance with the Act.

Privacy and Political Parties

2026-15: That government implement statutory privacy protections and independent oversight for personal information held by political parties.

Enhanced Safeguards for Sensitive Categories of Data

2026-16: Should government wish to introduce more prescriptive protections for specific categories of data, we would like to be consulted on the specific proposed language for such protections.

Rights of a Minor

No Recommendation

Indigenous Issues

2020.11.1: Initiate consultation with Indigenous organizations and governments in Newfoundland and Labrador, among other stakeholders such as the Intergovernmental and Indigenous Affairs Secretariat, to consider whether and how Indigenous organizations and governments could be referenced in the statute.

[Privacy Breach Notification Requirements and Timelines](#)

2026-17-1: Prescribe in the regulations the content that should be included when notifying affected individuals of a breach.

2026-17-2: Require breaches to be reported to the Minister responsible for ATIPPA, 2015 (as required by Alberta's POPA) and other interested parties (as required under PIPEDA). The breach reports should be done at the first reasonable opportunity.

[Public Body Breach Prevention, Response, and Reporting](#)

2026-18-1 (for Breach Prevention and Breach Response): Public bodies should have specific policies and procedures in place outlining what a privacy breach is and how to deal with it.

2026-18-2: Continued mandatory reporting of all breaches to OIPC.

2026-18-3: Amend section 64(4) of ATIPPA, 2015 to include reporting the privacy breach to the commissioner "at the first reasonable opportunity".

2026-18-4: Amend section 64(5) of ATIPPA, 2015 to allow the commissioner to "require" the head of the public body notify the individual.

[Privacy Management Frameworks](#)

2026-19: Require all public bodies to establish, implement, and maintain comprehensive Privacy Management Programs. If critical content is identified in regulations, it should differentiate between public bodies with different capacities, such as smaller municipalities, from larger public bodies with high volumes of sensitive personal information, such as the Department of Government Services.

[Privacy Impact Assessments](#)

2026-20-1: Require all public bodies to complete PIAs. The Minister responsible for the Act be required to maintain a comprehensive, up-to-date registry of PIAs, including a brief summary of all PIAs.

2026-20-2: Amend the Act to include a definition of "common or integrated program or service" similar to that of British Columbia.

2026-20-3: Include a provision in the Act that requires public bodies to submit a PIA to the Commissioner for review and comment upon the Commissioner's request.

2026-20-4: Add regulations that address critical PIA content, including requiring that PPIAs document why a full PIA is not recommended.

[Mandatory Training](#)

2026-21: Amend the Act to include a mandatory training requirement with clear obligations to track completion and ensure training is completed at regular intervals.

[Additional Oversight or Enforcement Mechanisms](#)

2026-22: If government considers the consultation requirements in section 112 to be insufficiently clear to facilitate the provision of draft bills to the Commissioner for review, section 112 should be amended to expressly require it.

[Duty to Document](#)

2026-23-1: Amend the Management of Information Act to legislate a Duty to Document for entities subject to that legislation, providing for OIPC oversight.

2026-23-2: Consider whether to broaden the scope of public bodies to which the Duty to Document would apply, to all public bodies subject to ATIPPA, 2015 except those that are subject to the Towns and Local Service Districts Act.