ombud
NEW BRUNSWICK • NOUVEAU-BRUNSWICK

2025 Legislative Review of the *Right to Information and Protection of Privacy Act*

Submission from the Ombud for New Brunswick

September 2025

ombud
NEW BRUNSWICK • NOUVEAU-BRUNSWICK

September 12, 2025

Hon. René Legacy, Minister
Finance and Treasury Board
Office of the Chief Information Officer
P.O. Box 6000
Fredericton, NB E3B 1E9

Subject: RTIPPA Review

Mr. Legacy,

I am pleased to provide you with my submission for the legislative review of the *Right to Information and Protection of Privacy Act ("RTIPPA").*

As the designated statutory oversight body under *RTIPPA*, and in keeping with the authorities afforded to me under subsection 64.1(1) of the *Act*, my office and I are uniquely positioned to provide an examination and recommendations regarding this *Act* with respect to areas requiring improvement. This submission reflects the observations borne of our experience in exercising these oversight obligations under *RTIPPA*, as well as research conducted on best practices observed in other provincial and territorial jurisdictions in Canada.

I look forward to participating in the on-going review process and would be pleased to discuss my submission at your convenience.

Cordially,

Marie-France Pelletier
Ombud for New Brunswick

ombudnb.ca

Tel. Tél. : (506) 453-2789 1-888-465-1100
Fax • Télécop. : (506) 453-5599**Email**
Courriel: ombud@ombudnb.ca

P.O. Box 6000 C.P. 6000
Fredericton, N.B. E3B 5H1

Table of Contents

PART 1 – Recommendations related to *RTIPPA*'s current provisions

Section 1 – Definitions

Expansion of the definition of "government body"

While *RTIPPA* applies to a wide array of public sector entities, **the current wording of the definitions leaves out some organizations that are closely linked to government operations.**

As an example, this office recently dealt with a question of whether an organization was a government body under *RTIPPA*.[1] Four of the organization's board members were senior government officials and the Province of New Brunswick had long been its majority shareholder. Despite these close ties, the organization did not meet the definition of a government body.

Section 1, *RTIPPA*

"government body" means

(a) any board, Crown corporation, commission, association, agency or similar body, whether incorporated or unincorporated, all the members of which, or all the members of the board of management or board of directors or governing board of which, are appointed by an Act of the Legislature or by the Lieutenant-Governor in Council, and

(b) any other body that is designated in Schedule A as a government body.

The criteria for government-related entities should be captured in *RTIPPA* to promote greater transparency and openness about government activities and their impact on public finances.

Saskatchewan and British Columbia's information and privacy laws specify that entities are subject to these laws where all or part of their members, officers, and/or directors are appointed by the government or a provincial law. Newfoundland and Labrador, Alberta, and British Columbia's laws also consider whether the government has a controlling interest or owns most of the share capital of an entity as a key factor. For example:

> Newfoundland and Labrador's *Access to Information and Protection of Privacy Act*:
>
> *2. In this Act*
> *(x) "public body" means*
>
> *…*
> *(ii) a corporation, the ownership of which, or a majority of the shares of which is vested in the Crown,*
> *(iii) a corporation, commission or body, the majority of the members of which, or the majority of members of the board of directors of which are appointed by an Act, the Lieutenant-Governor in Council or a minister*

[1] *New Brunswick (Natural Resources and Energy Development) (Re)*, 2024 NBOMBUD 6 (CanLII).

Recommendation 1

Amend the definition of "government body" in section 1 to expand it to:

- bodies whose majority of members, officers, and/or directors are appointed by an Act, a minister or the Lieutenant-Governor in Council; and
- those the government owns or in which it has a controlling interest.

Expansion of the definition of "personal information"

While the current definition of personal information provides an extensive list of the types of information captured by *RTIPPA*, **the development and use of new forms of personal information and technologies should be specifically addressed in *RTIPPA***.

One such example is facial recognition technology. This office has been consulted by local governments on its use for various purposes, including law enforcement. While we have not, to date, received complaints related to the use of such technologies, making specific reference to new forms of personal information would be well advised and in keeping with best practices in other jurisdictions.

Biometric information is included in the definition of personal information under information and privacy laws in Prince Edward Island, Alberta, and Yukon. For example:

> Alberta's *Access to Information Act*:
>
> *1 In this Act,*
> *(b) "biometric information" means information derived from an individual's unique measurable characteristics;*
> *(r) "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 […]*

Section 1, *RTIPPA*

"personal information" means recorded information about an identifiable individual, including but not limited to,

(a) the individual's name,
(b) the individual's home address or electronic mail address or home telephone or facsimile number,
(c) information about the individual's age, gender, sexual orientation, marital status or family status,
(d) information about the individual's ancestry, race, colour, nationality or national or ethnic origin,
(e) information about the individual's religion or creed or religious belief, association or activity,
(f) personal health information about the individual,
(g) the individual's blood type, fingerprints or other hereditary characteristics,
(h) information about the individual's political belief, association or activity,
(i) information about the individual's education, employment or occupation or educational, employment or occupational history,
(j) information about the individual's source of income or financial circumstances, activities or history,
(k) information about the individual's criminal history, including regulatory offences,
(l) the individual's own personal views or opinions, except if they are about another person
(m) the views or opinions expressed about the individual by another person, and
(n) an identifying number, symbol or other particular assigned to the individual.

Recommendation 2

Amend the definition of "personal information" in section 1 to include biometric information.

Definitions surrounding artificial intelligence

Artificial intelligence (AI) promises increased efficiencies and can be used to analyze and make decisions from large amounts of data. **Public sector organizations are increasingly considering how they can leverage AI to deliver public services, including in New Brunswick.**[2]

Part 3 of this submission explores some of the public policy considerations surrounding the use of AI in the public sector. One such issue is the necessity to define certain key terms in access to information and privacy legislation, recognizing that information collected or used through AI falls within the protections of this legislation.

Recommendation 3

Amend section 1 to define terms such as artificial intelligence, generative artificial intelligence, and automated decision-making.

Section 2 – Purposes of the Act

A purpose clause sets the overall spirit and intent of the law. It provides a useful lens through which to interpret legislative requirements.

New Brunswick's current purpose clause sets out the basic purposes of *RTIPPA*. It could go further to explain that access to information is a cornerstone of a transparent and accountable government and a key tool for citizens to be informed and knowledgeable when participating in the democratic process. The clause could also be used to explain that another key purpose of the legislation is to ensure the protection of privacy.

Some jurisdictions have adopted language that references the broader aims of access and privacy laws, such as facilitating democracy, meaningful participation in the democratic process,

Section 2, *RTIPPA*

2 The purposes of this Act are

(a) to allow any person a right of access to records in the custody or under the control of public bodies, subject to the limited and specific exceptions set out in this Act,
(b) to control the manner in which public bodies may collect personal information from individuals and to protect individuals against unauthorized use or disclosure of personal information by public bodies,
(c) to allow individuals a right of access to records containing personal information about themselves in the custody or under the control of public bodies, subject to the limited and specific exceptions set out in this Act,
(d) to allow individuals a right to request corrections to records containing personal information about themselves in the custody or under the control of public bodies, and
(e) to provide for an independent review of the decisions of public bodies under this Act.

[2] For example, in June 2025, *l'Acadie Nouvelle* published a series of articles on the use of AI in the law enforcement, university and municipal sectors in New Brunswick.

increasing transparency and accountability.[3] Other jurisdictions also reference the protection of privacy in their purpose clauses.

Recommendation 4

Amend the purpose clause in section 2 to reference democratic and transparency principles behind access to information and reinforce the importance of protecting privacy.

Section 4 – Records excluded from the application of the Act

> **Section 4, *RTIPPA***
>
> This Act does not apply to:
>
> (b) a record pertaining to legal affairs that relate to the performance of the duties and functions of the Office of the Attorney General

Overall, the classes of records excluded from the scope of *RTIPPA* are largely consistent with other Canadian jurisdictions. **The notable exception is paragraph 4(b) which excludes "a record pertaining to legal affairs that relate to the performance of the duties and functions of the Office of the Attorney General".**

At the time of its inclusion in *RTIPPA* in 2010, this was a novel exclusionary clause not found in comparable legislation across Canada. No other Canadian jurisdiction has followed suit in the 15 years since the introduction of this provision, and New Brunswick remains an outlier in this regard.

This office has received complaints over the years about the Office of the Attorney General invoking this provision to refuse access. For example, at one time, the Attorney General's Office had relied on paragraph 4(b) to refuse access to the amount of legal fees paid. One of my predecessors, former Commissioner Deschênes, found this was an overreach and that this matter would be better addressed under the section 27 legal privilege exception to disclosure.[4]

More recently, the Department of Justice and Public Safety relied on paragraph 4(b) to refuse access to an internal report about the impact of a Crown prosecutor shortage on the criminal justice system. The Department was invited to explain how it defines and interprets "legal affairs" when applying paragraph 4(b), given that the vagueness of the meaning of "legal affairs" had also been noted by the courts. Unfortunately, the Department did not provide submissions on this point.[5]

RTIPPA's section 27 already contains a legal privilege exception as follows:

---

[3] Examples of this can be found in Newfoundland and Labrador, Nova Scotia and Yukon's laws as well as in Canada's *Access to Information Act*.
[4] *New Brunswick (Attorney General) (Re)*, 2018 NBOMB 6 (CanLII).
[5] *New Brunswick (Justice and Public Safety) (Re)*, 2024 NBOMBUD 8 (CanLII).

27 Subject to paragraph 4(b) and section 22.1, the head of a public body may refuse to disclose to an applicant

(a) information that is subject to solicitor-client privilege,

(b) information prepared by or for an agent or lawyer of the Office of the Attorney General or the public body in relation to a matter involving the provision of legal advice or legal services or in relation to the investigation or prosecution of an offence, or

(c) information in a communication between an agent or lawyer of the Office of the Attorney General or the public body and any other person in relation to a matter involving the provision of legal advice or legal services or in relation to the investigation or prosecution of an offence.

Section 27 of *RTIPPA* is sufficiently broad to protect the legal work conducted by the Office of the Attorney General from disclosure. It does not appear that paragraph 4(b) serves any independent purpose to allow the Attorney General's Office to appropriately protect solicitor-client privileged information.

Recommendation 5

Repeal the paragraph 4(b) exclusion.

Section 5 – Prevailing clause

Section 5, *RTIPPA*

If a provision of this Act is inconsistent with or in conflict with a provision of another Act of the Legislature, the provision of this Act prevails unless the other Act of the Legislature expressly provides that it, or a provision of it, prevails despite this Act.

RTIPPA is intended to be the primary authority for access to information and privacy protection across the public sector. Over the years however, there has been a proliferation of other legislation adopted in New Brunswick that specifically state that they are to take precedence over right to information and privacy laws. **While the Legislative Assembly has the ultimate authority to decide the laws of the Province, if it only deals with prevailing clauses on a case-by-case basis, it may be doing so without a clear sense of the overall impact that these clauses may be having on access and privacy rights.**

The use of prevailing clauses is not unique to New Brunswick, and in some cases may be well justified. This office identified more than 70 acts and regulations with provisions that are intended to override *RTIPPA* in whole or part. This can only be found by looking at each individual act and regulation as *RTIPPA* does not currently require a comprehensive list of prevailing clauses.

The main concern is the number of clauses intending to prevail over *RTIPPA* that have been enacted since it came into force in 2010 and the lack of a process to review the effectiveness and necessity of such clauses.

Including a list of prevailing clauses in a schedule to RTIPPA would provide better transparency by showing the full picture of all the enacted prevailing clauses. It would also make it easier to identify applicable prevailing clauses by public bodies in their day-to-day work as well as this office when investigating complaints.

Newfoundland and Labrador requires that all prevailing clauses be listed in Schedule A of their access and privacy legislation. Further, the recurring legislative reviews of the law are to include a review of the provisions listed in Schedule A to determine the necessity for their continued inclusion.

Schedule A currently lists provisions under 24 acts and regulations as prevailing over the Act. The most recent review of the Newfoundland and Labrador law included a review of the existing prevailing clauses in Schedule A, which resulted in recommendations to government to maintain several of the prevailing clauses and to remove others.[6]

Recommendation 6

Amend *RTIPPA* by adding a Schedule to include a list of all legislative provisions that prevail over *RTIPPA* and specify that the contents of the said Schedule be subject to any review of *RTIPPA* initiated under section 86.1.

Section 11 – Time limit for responding

Timelines to respond to access requests

Public bodies routinely deal with requests that are broad in scope, including requests for any and all records about a particular topic, sometimes spanning several years. **An access request can be for a single record or thousands of pages of records, depending on what the applicant is seeking. For this reason, public bodies may sometimes require more time to be able to fully respond to an access to information request.**

When *RTIPAA* came into force in 2010, it required public bodies to respond to access to information requests within 30 calendar days. Public bodies could extend this timeline for specific reasons for an additional 30 days. Longer time extensions could only be approved by the oversight body.

Section 11, *RTIPPA*

11(1) The head of a public body shall respond in writing to a request for access to a record within 30 business days after receiving the request unless

(a) the time limit for responding is extended under subsection (3) or (4),

(b) the request has been transferred to another public body under section 13, or

(c) an estimate is given to the applicant under section 80.

11(3) The head of a public body may extend the time for responding to a request for up to an additional 30 business days if […]

11(4) In any case referred to in subsection (3), the head of a public body may, if approved by the Ombud, extend the time limit for responding to a request for a period longer than 30 business days.

In April 2018, the timelines to respond to access requests were changed from calendar to business days. This gave public bodies more time to respond to access requests, moving the initial response time from 30 calendar days to 30 business days

[6] ATIPPA Statutory Review Committee 2020, Final Report (June 8, 2021): https://www.nlatippareview.ca/files/FINAL-REPORT-June-8-2021-2.pdf

(approximately one and a half months). If public bodies self-extend this deadline, the total time to respond could be up to 60 business days (approximately three months).

New Brunswick was one of the first jurisdictions in the country to set a timeline to respond to access requests beyond 30 calendar days. Manitoba and Alberta have since followed suit, with Manitoba's initial timeline being 45 calendar days and Alberta's 30 business days. Nunavut also allows public bodies 25 business days to respond. Most other jurisdictions in the country set an initial timeline to respond to requests at 30 calendar days, except for Quebec, which leads the country with 20 calendar days.

Since this office only deals with time extension applications from public bodies asking for additional time to respond to access requests beyond 60 business days, we do not have data to assess the overall impact of the longer timelines that were introduced in 2018. Ideally, public bodies should be using the additional time to provide more fulsome responses to access requests.

Recommendation 7

Assess the impact of the extended timelines on public bodies' ability to provide timely and fulsome responses to access to information requests and reconsider the timelines to align with the standards set out in most other Canadian jurisdictions.

Section 15 – Power to disregard access requests

Section 15, *RTIPPA*

15 On the request of a public body, the Ombud may authorize the head to disregard one or more requests for access if the request for access

(a) would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the request or previous requests,

(b) is incomprehensible, frivolous or vexatious, or

(c) is for information already provided to the applicant.

Authority to disregard requests

Public bodies cannot disregard access to information requests themselves and must apply to this office for permission to do so. All but four Canadian jurisdictions have similar provisions to those that currently exist in New Brunswick.

The four jurisdictions that allow a public body to disregard or refuse to process an access request themselves are Ontario, Manitoba, Alberta, and Yukon. Yukon's legislation has an added feature that confers an obligation for the public body to consult with the applicant prior to deciding to disregard their access request. This provides an opportunity for the applicant to be heard before the public body decides to refuse to process or disregard an access to information request.

It is preferable to have an independent review process before removing access rights under *RTIPPA*. The main benefit of involving the oversight body during the initial processing of the request is that the public body's concerns can be addressed sooner without putting the burden on the applicant to take the additional step of filing a complaint if a public body were able to unilaterally disregard a request.

Recommendation 8

Maintain the oversight role of the Ombud on requests to disregard an access to information request under *RTIPPA*.

Inconsistencies between English and French wording

The current wording of paragraph 15(a) does not say the same thing in English and in French. It should be revised for clarification and consistency. Paragraph 15(a) provides criteria to consider prior to disregarding an access to information request. The English version states:

> *"would unreasonably interfere with the operations of the public body because of the repetitious or systematic nature of the request or previous requests"*

The French version states :

> *"la demande nuirait déraisonnablement aux activités de l'organisme ou serait abusive en raison de leur caractère répétitif ou systématique"* [emphasis added]

The notion of the "abusive nature" of a request is absent from the English version. All Canadian jurisdictions have disregard provisions in their respective access to information laws and most all of them have language about the abuse of access rights as grounds to disregard requests. While most applicants exercise their access rights in good faith, consideration should be given to which version of the current s. 15 best reflects the legislative intent.

Recommendation 9

Amend paragraph 15(a) to ensure the English and French versions have the same meaning and effect.

Process improvements for requests to disregard

While *RTIPPA* gives this office the power to allow a public body to disregard an access request, it is silent on the process by which to do it. **Other Canadian jurisdictions have laid out comprehensive processes for requests to disregard.**

Section 11 of *RTIPPA* gives this office the power to approve time limit extensions for public bodies to respond to an access to information request in certain circumstances. *RTIPPA* requires the public body to write to the applicant to let them know the reason for the extension and when to expect the public body's response.

A similar process could be used for requests to disregard. For example, when this office has authorized a public body to set aside an access to information request, the public body would be required to send the applicant a written notice explaining:

- why the request was disregarded,
- that the Ombud has approved this decision, and
- advise of any recourse or appeal rights.

This type of process is currently in place in Newfoundland and Labrador and in Nova Scotia.

Consideration should also be given to setting timelines within this process. The Newfoundland and Labrador right to information laws requires public bodies to submit disregard applications to the oversight body within five business days of receiving the access to information request. Nova Scotia requires this be done within 14 days of receipt of a request.

As for the timing of the oversight body's decision, the Newfoundland and Labrador legislation requires the oversight body to decide within three business days of receiving the public body's disregard application. Nova Scotia requires this be done within 14 days of receipt.

Whether processing the access to information requests should be put on hold when public bodies seek authorization to disregard them is also worthy of exploring.

Of the ten jurisdictions across Canada where public bodies have to seek oversight approval to disregard access requests, five place the processing of the request on hold pending the oversight body's decision.[7] The other five, including New Brunswick, do not place the processing of the request on hold, meaning that the disregard process has to unfold within the public body's statutory time limit to respond.[8]

Finally, disregarding or setting aside an access to information request is a serious matter, as it removes the applicant's rights. Consideration should be given to creating a statutory right of appeal to the courts for the applicant when an access request is disregarded, like in Newfoundland and Labrador and in Nova Scotia.[9]

---

[7] This is the case in Nova Scotia, Prince Edward Island, British Columbia, Saskatchewan, and Canada's *Access to Information Act*.
[8] This is the case in Newfoundland and Labrador, Quebec, Northwest Territories, and Nunavut.
[9] See paragraph 21(6)(c) of the Newfoundland and Labrador *Access to Information and Protection of Privacy Act, 2015*, and paragraph 6E(c) of the Nova Scotia's *Freedom of Information and Protection of Privacy Act*.

Recommendation 10

Amend *RTIPPA* to improve the processes for disregarding access to information requests, namely:

- a requirement to notify applicants when an access request has been set aside;
- time limits to file and render decisions for applications to disregard;
- clarifying the requirement to process access to information requests pending a decision on disregarding the request; and
- allowing the applicant to appeal to the courts when an access request is disregarded by a public body.

Section 17 - Mandatory exception to disclosure

Executive Council confidences

Executive Council (Cabinet) confidences are a long-held tradition in parliamentary democracies that encourage ministers to speak freely at the Cabinet table without fear that what they say will be made public. The goal is to allow a government to thoroughly examine all aspects of an issue in private, while speaking with one voice and being accountable as a group for their decisions once made public.

While Cabinet confidences and solidarity are a foundational principle and cornerstone of good governance, the current protection offered by section 17 can lend itself to an overly broad interpretation and blanket refusals of any Cabinet-related information on principle.

This raises the question of how the core principles and purposes of Cabinet confidences can remain protected, as needed, while allowing for greater transparency and accountability in government decision-making.

One option to consider is the approach taken in the United Kingdom and New Zealand. Instead of a broad protection of all Cabinet-related information, their respective access to information laws have taken a harms-based approach, allowing information to be protected if disclosure would be injurious to the following interests:

- the convention of collective ministerial responsibility,
- the frankness and candour of Cabinet discussions, or

Section 17, *RTIPPA*

Executive Council confidences

17(1) The head of a public body shall refuse to disclose to an applicant information that would reveal the substance of deliberations of the Executive Council, including but not limited to,

(a) an agenda, minute or other record of the deliberations or decisions of the Executive Council,

(b) discussion papers, policy analyses, proposals, memorandums, advice or similar briefing material submitted or prepared for submission to the Executive Council,

(c) a proposal or recommendation prepared for, or reviewed and approved by, a Minister of the Crown for submission to the Executive Council,

(d) a record that reflects communications among Ministers of the Crown relating directly to the making of a government decision or the formulation of government policy, and

(e) a record prepared to brief a Minister of the Crown about a matter that is before, or is proposed to be brought before, the Executive Council or that is the subject of communications referred to in paragraph (d).

17(2) With the approval of the Executive Council, the Clerk of the Executive Council may disclose information referred to in subsection (1) if a record is more than 15 years old.

- the efficiency of the Cabinet's decision-making process.[10]

Moving from a mandatory full exclusion to withholding information only where necessary could help strike a better balance between safeguarding Cabinet deliberations, where appropriate, and supporting the public's right to know more about the decisions made by its government.

Another option to consider is found in several jurisdictions in Canada[11] as well as the United Kingdom and Australia. These jurisdictions have adopted "public interest override" provisions that apply to Cabinet confidences. A public interest override clause recognizes that there may be circumstances where information that normally would be protected should be made known to the public. This would require a balancing of the public interest in disclosure against the interest in non-disclosure to protect Cabinet confidences.

See, for example, subsection 27(3) of the Newfoundland and Labrador legislation:

> *(3) Notwithstanding subsection (2), the Clerk of the Executive Council may disclose a cabinet record or information that would reveal the substance of deliberations of Cabinet where the Clerk is satisfied that the public interest in the disclosure of the information outweighs the reason for the exception.*

Finally, another option to consider lies in allowing some limited disclosure of information contained in Cabinet documents. For example, the Newfoundland and Labrador legislation specifically excludes factual or background information in the definition of "Cabinet record" under paragraph 27(1)(d):

> *27. (1) In this section, "cabinet record" means*
>
> > *(d) a discussion paper, policy analysis, proposal, advice or briefing material prepared for Cabinet, excluding the sections of these records that are factual or background material*; [emphasis added]

Yukon has a similar exclusion and allows for the disclosure of factual information and background explanations or analyses to be disclosed in certain circumstances.

> Yukon's *Access to Information and Protection of Privacy Act*:
>
> *67(2) For the purpose of the definition "Cabinet record" in subsection (1), information of the following types is not considered to be a Cabinet record or a part of a Cabinet record:*

---

[10] See *Freedom of Information Act 2000* (UK), c. 36, ss. 36(2) (Prejudice to effective conduct of public affairs) and *Official Information Act 1982*,(NZ) 1982/156, paras. 9(2)(f) and 9(2)(g) (Other reasons for withholding official information).

[11] See legislation in Newfoundland and Labrador, Nova Scotia, Prince Edward Island, Alberta, British Columbia, and Yukon.

(a) factual information included in a Cabinet record only for the purpose of providing contextual background information;

(b) information included in a Cabinet record for the purpose of providing Cabinet with a background explanation or analysis for its consideration in making a decision but only if

(i) the decision has been made public,
(ii) the decision has been implemented, or
(iii) five years or more have passed since the decision was made or the matter considered by Cabinet;

(c) information in a Cabinet record that reflects the decision of Cabinet in respect of an appeal brought before it under an Act.

Recommendation 11

Amend *RTIPPA* to allow for a broader disclosure of Cabinet records.

Historical Cabinet records

Currently, the Executive Council confidences exception in section 17 of *RTIPPA* creates a mandatory 15-year ban on making this information publicly available. Although the government holds the Cabinet confidences privilege, there is no option for it to choose to disclose this kind of information, even if there were a compelling reason to do so.

As such, New Brunswick has one of the most restrictive exceptions to disclosure for historical Cabinet records, which can only be disclosed with Cabinet approval despite being more than 15 years old. **According to the current wording of the *Act*, all historical Cabinet records could be withheld indefinitely if Cabinet declines to exercise its discretion in favour of disclosure.**

Other Canadian jurisdictions do not restrict disclosure or require Cabinet approval once a certain number of years has passed, the range being between 10 to 25 years.

Recommendation 12

Remove the requirement in subsection 17(2) for Executive Council approval for disclosure after 10 years.

Section 21 – Unreasonable invasion of third party's privacy

During this office's complaint investigations, we have noted an often well-intentioned but overzealous application of *RTIPPA*'s section 21. Public bodies are aware of the need to protect privacy, including during the processing of access to information requests, and some have taken the approach that if it appears to be third party personal information of any kind, it should be withheld or redacted.

The section 21 exception contains two deeming clauses at subsections 21(2) and (3) that set out circumstances in which disclosure of third-party personal information is deemed to be, or not be, an unreasonable invasion of privacy. **The examples listed in subsections 21(2) and (3) are helpful when one of these specific circumstances applies; however, the list is not exhaustive and does not provide any guidance or direction if none of the listed examples apply.**

On this point, nearly all other Canadian jurisdictions' respective exceptions set out a list of factors to consider in determining whether disclosure would be an unreasonable invasion of privacy. For example, the Newfoundland and Labrador statute provides:

> *40(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether*
> *(a) the disclosure is desirable for the purpose of subjecting the activities of the province or a public body to public scrutiny;*
> *(b) the disclosure is likely to promote public health and safety or the protection of the environment;*
> *(c) the personal information is relevant to a fair determination of the applicant's rights;*
> *(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;*
> *(e) the third party will be exposed unfairly to financial or other harm;*
> *(f) the personal information has been supplied in confidence;*
> *(g) the personal information is likely to be inaccurate or unreliable;*
> *(h) the disclosure may unfairly damage the reputation of a person referred to in the record requested by the applicant;*
> *(i) the personal information was originally provided to the applicant; and*
> *(j) the information is about a deceased person and, if so, whether the length of time the person has been deceased indicates the disclosure is not an unreasonable invasion of the deceased person's personal privacy*.

Adopting a provision to this effect in New Brunswick would provide guidance to public bodies struggling with how to assess possible unreasonable invasions of privacy while processing access to information requests and may reduce complaints on this point.

Recommendation 13

Amend section 21 to include factors to consider in determining when the disclosure of personal information would and would not be an unreasonable invasion of privacy.

Section 22 – Disclosure harmful to a third party's business or financial interests

The third-party business information exception under section 22 requires public bodies to protect certain kinds of information about third party companies and organizations. The purpose of the exception is to guard against the disclosure of sensitive information that would likely be harmful to third party business interests.

If information is a trade secret or the public body can show that the information was provided by a third party and that the third party considered it confidential, the harm in disclosure is presumed and there is no need for a separate harms assessment.

We have observed in complaint investigations that companies often claim that much, if not all, of the information about or relating to their business is confidential as a matter of principle, without considering or explaining how disclosure would likely harm their interests. Public bodies sometimes choose to go along with the company's objections, even though this might protect more information than *RTIPPA* allows.

This raises concerns that the current wording and application of section 22 is undermining openness and transparency in public body-private sector contracting.

Several Canadian jurisdictions[12] adopted a three-part harms test that requires public bodies to show that:

- the information is one of the protected kinds of information (trade secret, commercial, financial, scientific, technical or labour relations info),
- the information was supplied by the third party to the public body in confidence, **and**
- disclosure could reasonably be expected to result in the types of harm specified in the provision.

Adopting a three-part harms test would create a higher test to be met to protect third party business information and allow for greater transparency. It would also bring *RTIPPA* more in line with other Canadian jurisdictions that have long taken this approach.

Recommendation 14

Amend section 22 to create a three-part harms-based test.

Section 26 – Advice to a public body

Paragraph 26(2)(a), *RTIPPA*

26(2) Subsection (1) does not apply if the information

(a) is in a record that is more than 20 years old,

With regards to the disclosure of advice to a public body, *RTIPPA*'s paragraph 26(2)(a) provides that the exception applies to records that are less than 20 years old. **This protection for advice to a public body is longer than the blanket protection afforded to Cabinet records under section 17, which is currently 15 years.**

[12] See Newfoundland and Labrador, Nova Scotia, Prince Edward Island, Ontario, Alberta, British Columbia and Yukon.

In other Canadian jurisdictions, the blanket protection ranges from five years in Nova Scotia to 25 years in Saskatchewan.

Recommendation 15

Amend paragraph 26(2)(a) to reduce the blanket protection for all records related to advice to public bodies to make it consistent with the protection afforded to Cabinet records under section 17.

Section 70 – Production of records

Subsection 70(1), *RTIPPA*

70(1) With the exception of Executive Council confidences and any document that contains information that is subject to solicitor-client privilege, the Ombud may require any record in the custody or under the control of a public body that the Ombud considers relevant to an investigation to be produced to the Ombud and may examine any information in a record, including personal information.

At this time, this office's powers to compel the production of records do not extend to Cabinet confidences and solicitor-client privilege. **New Brunswick is currently one of two Canadian jurisdictions with these express statutory restrictions on the oversight body's authority to require the production of records.**[13]

Despite this gap, some public bodies have had no issue with allowing this office to review such records. In some cases, public bodies have agreed to provide a list of the records at issue that gives sufficient detail to assess whether they have made a *prima facie* case that the claimed exception applies. Nonetheless, there are a small number of public bodies that have declined to provide any information for our review. In situations involving solicitor-client privilege, the questions raised by some of these public bodies stems from concerns that disclosing even a list of records could be interpreted as a waiver of privilege that could negatively affect their legal position in the matters at issue.

On this point, some jurisdictions[14] have adopted provisions in their legislation to specify that providing such records to the Commissioner (in our case the Ombud) during investigations does not constitute a waiver of solicitor-client privilege.

While the Ombud has powers under the *Inquiries Act*, the remedies provided in that *Act* (fines and/or imprisonment) would be inadequate to compel the production of records for our review. Under subsection 38(3) of the Nova Scotia *Freedom of Information and Protection of Privacy Act*, the Commissioner can apply to the Supreme Court of Nova Scotia for a production order if a public body does not comply with the requirement to produce records for the Commissioner's examination.

---

[13] Alberta recently became the second jurisdiction. See section 50 of the *Access to Information Act* that came into force in June 2025.
[14] See British Columbia's *Freedom of Information and Protection of Privacy Act*, ss, 44(2.1) and Yukon's *Access to Information and Protection of Privacy Act*, s. 98.

Recommendation 16

Amend *RTIPPA* by:

- removing the exception for Executive Council confidences and solicitor-client privilege found in subsection 70(1)
- specifying that production of information or a record to the Ombud for review does not constitute a waiver of legal privilege
- allowing the Ombud to apply to the courts for an order for the production of records.

PART 2 – Recommendations related to *RTIPPA*'s *General Regulation*[15]

Section 4.2 – Information practices

Subsection 4.2(1), *General Regulation - RTIPPA*

4.2(1) The following definitions apply in this section.

"privacy breach" means any incident of unauthorized access, use, disclosure or disposal of personal information in the custody of or under the control of a public body.

Expansion to the definition of privacy breach to include lost or stolen information

There is currently a gap in the definition of privacy breach. **In its current form, the definition does not include lost or stolen personal information.** Lost or stolen personal information is considered to be a privacy breach in other Canadian jurisdictions. Lost or stolen personal health information is also considered a privacy breach under New Brunswick's *Personal Health Information and Privacy Act*.

Recommendation 17

Amend the definition of "privacy breach" in section 4.2 to include circumstances where personal information has been lost or stolen.

Sections 5 and 7 – Referrals and Appeals to the Court of King's Bench

Notifying the Office of the Ombud of court referrals, appeals, and decisions

If someone is not satisfied with how a public body handled an access to information request, they may refer the matter to the courts instead of making a complaint to this office. When this occurs, *RTIPPA* does not set out a requirement to advise this office of the referral. It also does not require that this office be advised when a public body's decision to not follow a recommendation is appealed to the court.

As the oversight body, it is essential that this office be aware when questions about the interpretation and application of the law are before the courts and have access to court decisions that may not always be published and readily available. A requirement to notify this office would ensure up-to-date knowledge of the concerns and issues being brought before the courts and how *RTIPPA* is being interpreted.

Recommendation 18

Amend the *General Regulation* to require notifying the Ombud of referrals and appeals to the court and that court decisions be provided to the Ombud.

[15] Regulation 2010-111 made under section 85 of *RTIPPA*.

Procedure for appeals initiated by the Ombud

When a public body decides not to accept a recommendation made by the Ombud on an access to information or correction of personal information matter, the applicant has the right to file an appeal before the courts.

Where an applicant decides not to exercise their appeal rights, the law gives the Ombud the option to appeal of their own initiative.

While section 75 of *RTIPPA* states that this office can appeal a matter "in accordance with the regulations", **the regulations do not include the process for an appeal filed by this office or a prescribed appeal form for this office.**

This can be remedied by adding a process for appeals filed by this office and creating a separate appeal form, as is provided for the other court processes under the *Act*.

Recommendation 19

Amend the *General Regulation* to include a process for appeals filed by the Ombud, and add a prescribed form for appeals initiated by the Ombud.

PART 3 – Recommendations related to other public policy issues

Areas of improvement to the Ombud's powers under *RTIPPA*

Consultation with the Ombud on draft legislation that could impact access or privacy rights

The Ombud currently has the power to comment on the implications for access to information or the protection of privacy of proposed legislative schemes. **However, there is no formal requirement for government to consult the Ombud and engage this office's expertise on potential access and/or privacy implications of proposed laws before they are tabled in the Legislative Assembly.**

While not a consistent requirement across the country, the Newfoundland and Labrador law has made this a requirement:

> *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.*

Recommendation 20

Enact a requirement for public bodies to consult with the Ombud on draft laws that could have implications for access to information or protection of privacy.

Intervenor status in court referrals and appeals

In Part 2 of this submission, we discussed amendments to the *General Regulation* related to court referrals and appeals. **Another important public policy issue to consider is establishing a proactive role for the Ombud by granting the position intervenor status before the courts.** This was recommended originally by one of the Ombud's predecessors, former Commissioner Deschênes, in his 2018 Annual Report.[16]

While it would likely not be necessary for this office to exercise this right in every case, having intervenor status would allow this office to meaningfully participate in court hearings by providing its well-established and long-standing expertise on the

[16] https://oic-bci.ca/wp-content/uploads/2019/01/Final-Annual-2017-2018-ENG.pdf at p. 30.

interpretation and application of the law that may not otherwise be available to the court through the parties' submissions.

This office has successfully applied and been granted status as *amicus curiae* ("friend of the court") in a previous matter to provide insight into investigation and appeal procedures under *RTIPPA.* Having automatic intervenor status would simplify the process by dispensing with the need to file motions asking for this status on a case-by-case basis.

Such a precedent exists in Newfoundland and Labrador and Yukon's laws that grant the oversight body the power to intervene in a court appeal where a public body does not comply with or rejects the oversight body's recommendations.

Recommendation 21

Amend *RTIPPA* to create a statutory right for the Ombud to intervene in court referrals and appeals.

Recommendation vs. order-making powers

The question of whether an access and privacy oversight body should have recommendation or order-making powers is often raised during legislative reviews. Some hold the view that a recommendation power is a soft power, as public bodies can decide not to accept and follow oversight recommendations without any further consequence. An order-making power, while more binding, also requires additional procedures and resources. The accessible nature of complaints made to this office would transform into a more rigid process, similar to one before the courts, if it were to have order-making powers.

The question of recommendation vs. order-making powers was raised in the 2014 legislative review of the Newfoundland and Labrador legislation. It resulted in a third option: **a hybrid oversight model**. In that province, the Commissioner has a power of recommendation. However, if a public body decides not to accept the Commissioner's recommendations, it must apply to the court for a declaration that the recommendation need not be followed. This **removes the burden from the applicant, who may find it intimidating and expensive to have to go to the courts if they want a recommendation to be enforced**. Newfoundland and Labrador's legislation reads as follows:

> *50. (1) This section applies to a recommendation of the commissioner under section 47 that the head of the public body*
>
> *(a) grant the applicant access to the record or part of the record; or*
>
> *(b) make the requested correction to personal information.*
>
> *(2) Where the head of the public body decides not to comply with a recommendation of the commissioner referred to in subsection (1) in whole or in part, the head shall, not later than 10 business days after receipt of that recommendation, apply to the Trial Division for*

a declaration that the public body is not required to comply with that recommendation because

(a) the head of the public body is authorized under this Part to refuse access to the record or part of the record, and, where applicable, it has not been clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception;

(b) the head of the public body is required under this Part to refuse access to the record or part of the record; or

(c) the decision of the head of the public body not to make the requested correction to personal information is in accordance with this Act or the regulations.

(3) The head shall, within the time frame referred to in subsection (2), serve a copy of the application for a declaration on the commissioner, the minister responsible for the administration of this Act, and a person who was sent a copy of the commissioner's report.

(4) The commissioner, the minister responsible for this Act, or a person who was sent a copy of the commissioner's report may intervene in an application for a declaration by filing a notice to that effect with the Trial Division.

(5) Sections 57 to 60 apply, with the necessary modifications, to an application by the head of a public body to the Trial Division for a declaration.

The Newfoundland and Labrador legislation has the same process for recommendations made on privacy complaints.[17] This is an innovative approach to give more force and effect to the oversight body's recommendation powers. Rather than deciding not to accept a recommendation and waiting to see if an appeal is made to the courts, this instead requires the public body to take decisive action and make a case before the courts if it does not agree with the oversight body's recommendations.

Recommendation 22

Adopt a hybrid model, maintaining the Ombud's recommendation powers and instituting a requirement for public bodies to obtain a court order to set aside recommendations made by the Ombud on access to information or privacy matters.

Artificial intelligence

The use of artificial intelligence is a rapidly advancing area that needs careful consideration. **Given that these systems often involve personal information and can be used to make decisions that impact people's rights, AI in a public sector context raises important privacy concerns, as well as questions on how it should be regulated.**

In Canada, the federal government implemented a Directive on Automated Decision-Making[18] in 2019. The Directive's preamble states that the "government is committed to

[17] See section 79 in the Newfoundland and Labrador legislation.

[18] Government of Canada, Directive on Automated Decision-Making: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

using artificial intelligence in a manner that is compatible with core principles of administrative law such as transparency, accountability, legality, and procedural fairness." The federal Directive also sets out several requirements for the use of automated decision-making and artificial intelligence by federal departments and agencies.

While a directive is a useful guidance tool, it does not have the same force and effect as legislation. In 2021, the Privacy Commissioner of Canada called for the following changes[19] to the federal *Privacy Act*, which governs the handling of personal information in the federal public sector:

- The law should define automated decision-making.
- The law should include a right to meaningful explanation and human intervention related to the use of automated decision-making, as currently supported by the Treasury Board Secretariat's Directive on Automated Decision-Making.
- A specific standard should be set for the level of explanation required, so as to allow individuals to understand:
  (i) the nature of the decision to which they are being subject and the relevant personal information relied upon, and
  (ii) the rules that define the processing and the decision's principal characteristics.
- Where trade secrets or security classification prevent such an explanation from being provided, the following should at least be provided:
  (i) the type of personal information collected or used,
  (ii) why the information is relevant, and
  (iii) its likely impact on the individual.
- The law should contain an obligation for institutions to log and trace personal information used in automated decision-making.

Provincial oversight bodies in Newfoundland and Labrador, Nova Scotia, Alberta, and British Columbia have since called for similar changes to their respective public sector access and privacy laws.

In December 2023, Canadian privacy oversight bodies, including this office, jointly released "Principles for responsible, trustworthy and privacy-protective generative AI (artificial intelligence) technologies".[20] The oversight bodies noted that while generative AI tools may pose new risks to privacy and concerns about the collection, use, and

---

[19] Office of the Privacy Commissioner of Canada, *Submission of the Office of the Privacy Commissioner of Canada to the Minister of Justice and Attorney General of Canada: Public Consultation on Modernization of the Privacy Act*: https://www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103.

[20] Principles for responsible, trustworthy and privacy-protective generative AI technologies: https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai.

disclosure of personal information, they do not fall outside of current legal frameworks and must comply with Canadian privacy laws.

Earlier this year, the Chief Information Officer (CIO) for the Province surveyed employees in the public service to understand the impact of AI on their work. Employee responses outlined that there is interest in learning and building digital skills, comfort levels vary across teams and roles, and they want clear, practical guidance and support.

In providing initial survey results to employees of the public service, the CIO confirmed that they are "exploring how to approach emerging technologies like AI in a way that reflects the values of the public service and meets real needs in practice." A way in which to do so is to provide a legal framework that would serve to protect the rights and also reassure the public about the responsible handling of their personal information.

Recommendation 23

Amend *RTIPPA* to provide a legal framework to define:

- the rights and standards related to the handling of personal information involved in automated decision-making schemes;
- appropriate safeguards and rights for New Brunswickers in the creation and use of automated decision-making schemes by public bodies.

Duty to document

In 2016, Federal, Provincial, and Territorial Information and Privacy Commissioners (FPT Commissioners) issued a joint Statement on the Duty to Document.[21] The FPT Commissioners Statement indicates that a legislated duty to create records related to the key actions and decisions of public entities should be established. FPT Commissioners were also of the view that such a duty to document should be accompanied by oversight and enforcement provisions.

To date, British Columbia is the only Canadian jurisdiction that has implemented a duty to document through its *Information Management Act*. The legislation stipulates that "*the head of a public body […] is responsible for creating and maintaining […] government information that is an adequate record of the government body's decisions.*"[22]

---

[21] *Statement of the Information and Privacy Commissioners of Canada on the Duty to Document* (January 25, 2016): https://www.oic-ci.gc.ca/en/statement-information-and-privacy-commissioners-canada-duty-document

[22] See subsection 19(1) of the British Columbia legislation.

A legislated duty to document has also been implemented in jurisdictions such as New Zealand and some Australian states. These requirements are typically included in a public records law or its equivalent. Oversight over these matters rests with their Chief Archivist or equivalent entity.

A legislated duty to document key actions and decisions should be implemented in New Brunswick. Such a requirement **supports good governance and accountability, ensures the existence of an historical record for current and future generations, and reinforces the democratic principles upon which access to information rights are predicated.**

Recommendation 24

Create a legislated duty requiring public bodies to document matters related to key actions and decisions, along with oversight and enforcement provisions.

Exceptions to disclosure

Public interest override clause

RTIPPA does not contain a general requirement for public bodies to consider whether the public interest in having access to certain information outweighs the protection of the information from being released. Such a requirement is called a public interest override clause.

The only public interest override provisions in *RTIPPA* are found in subsections 22(4) and (5) for third party business information and a mandatory disclosure requirement under section 33.1 that is limited to disclosure of "*information about a risk of significant harm to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.*"

Several other Canadian jurisdictions have general public interest override clauses, though they vary in scope and application.

Newfoundland and Labrador and Ontario have general public interest override provisions, but they only apply to certain discretionary exceptions to disclosure. Newfoundland and Labrador's law also includes a public interest override specifically for Cabinet records and related information.

Several other jurisdictions have adopted general public interest disclosure provisions that apply despite any other provision of their law, including mandatory exceptions to disclosure.

Considering whether the public interest in disclosing information clearly outweighs the public interest in withholding the information from disclosure should form part of the analysis required in each access to information request, regardless of whether or not *RTIPPA* requires it. An important difficulty in doing so is that public interest remains a subjective term whose interpretation may vary depending on the perspective of those involved in a matter at issue.

Some jurisdictions have issued guidance on the interpretation and application of public interest disclosure.

One jurisdiction (Yukon) has codified the factors that a public body must consider in assessing public interest disclosure in its legislation. These factors include:

- the level of public interest in the information,
- whether the information is likely to be accurate and reliable,
- whether similar information is in the public domain,
- whether suspicion is likely to exist in respect of a public body's conduct in relation to the matter to which the information relates,
- if harm to a person, public body or government is likely to result from disclosure of the information, the significance and type of the harm, and
- whether the disclosure of the information is likely to result in similar information no longer being supplied to a public body.

In two other jurisdictions (Newfoundland and Labrador and Ontario), Information and Privacy Commissions have issued guidance documents or decisions to assist in assessing public interest disclosure.[23] These instruments can be useful to assist public bodies in New Brunswick in making their own determinations as to public interest disclosures.

Recommendation 25

Enact a general public interest override clause for all discretionary exceptions to disclosure and include a list of factors to consider in assessing public interest disclosure.

Records made by or for an officer of the Legislative Assembly

Currently, legislative officers are not defined as public bodies subject to *RTIPPA*. Further, paragraph 4(f) excludes all records made by or for an officer of the Legislative Assembly from the scope of the *Act*. This means that legislative officers, including this

[23] Office of the Information and Privacy Commissioner of Newfoundland and Labrador, *Guidelines for Public Interest Override* (last revised: March 31, 2023): https://www.oipc.nl.ca/files/GuidelinesPublicInterestOverride.pdf; Office of the Information and Privacy Commissioner of Ontario, *Interpretation Bulletin: Public Interest Override* (March 2024): https://www.ipc.on.ca/en/resources/interpretation-bulletins/public-interest-override.

office, are not required to follow the access and privacy obligations under *RTIPPA* and records made by or for these offices held by public bodies are not subject to the *Act*.

The question of whether legislative officers should be subject to *RTIPPA* is worthy of consideration and public debate, keeping in mind their unique nature and fundamental differences with the executive branch of government.

Legislative officers are key institutions of the legislative branch of government, founded in the Westminster model of parliamentary government. Legislative officers serve a crucial role in holding the executive branch of government to account to both the Legislature and the general public.

Legislative officers, as well as their respective roles and powers, are created by statute. They are independent of the executive branch of government by design and are accountable and report directly to the Legislative Assembly, which has the power to remove them from their positions only in serious circumstances.

RTIPPA defines officers of the Legislative Assembly as "the Speaker of the Legislative Assembly, the Clerk of the Legislative Assembly, the Chief Electoral Officer, the Ombud, the Child, Youth and Senior Advocate, the Consumer Advocate for Insurance, the Integrity Commissioner and the Auditor General."

In performing the duties and functions under their respective mandates, legislative officers are routinely entrusted with sensitive information, including personal information. Handling this information appropriately at all times is key to maintaining public trust in and accountability for legislative officers.

While much of the work that legislative officers do to fulfill their respective mandates requires a high degree of confidentiality and there are good reasons why they are not currently subject to *RTIPPA*, there may also be benefits to having certain aspects of their operations subject to possible public disclosure. That being said, careful consideration is needed before taking such a step.

Just as *RTIPPA* provides a standard set of principles to promote transparency and accountability across the public sector, similar considerations must be made with respect to the unique role and function that legislative officers serve to ensure that the sensitive nature of their work is appropriately protected and safeguarded as needed.

Currently across Canada, several jurisdictions exclude statutory officers from the scope of their respective access and privacy laws, but this is not the case everywhere. Five jurisdictions across the country treat legislative or statutory officers as public bodies under their respective access and/or privacy laws.[24]

---

[24] See Newfoundland and Labrador, Prince Edward Island, Alberta, British Columbia and at the federal level.

In looking at their respective laws, each jurisdiction turned its mind to the unique and specific functions that legislative officers serve and has enacted related provisions to safeguard the more sensitive aspects of their work. Each jurisdiction has taken its own approach to these concerns, which includes enacting exceptions to disclosure that are specific to legislative officers collectively, and/or individually, and/or creating specific carve outs, meaning that their respective laws do not apply to certain kinds of information created by or for or relating to legislative officers' statutory functions.

In each of these jurisdictions, the access and/or privacy oversight body serves as the oversight body for the other legislative officers. This office is poised to take on the oversight role relative to our fellow legislative officers should the scope of *RTIPPA* be expanded.

For obvious reasons, a different solution would be needed if this office were to be made subject to *RTIPPA*. While the Newfoundland and Labrador and federal statutes are silent on this point, the Prince Edward Island, Alberta and British Columbia legislation allow for either the responsible Minister or the Lieutenant Governor-in-Council to order or designate a judge to act as adjudicator for complaints or concerns about the Information and Privacy Commissioner's decisions and actions as a public body under their respective laws.

Recommendation 26

Ensure that the following steps be taken before deciding on the expansion of *RTIPPA* to legislative officers:

- consult with each legislative officer to identify and explore any mandate-specific concerns they may have, including existing statutory confidentiality and public disclosure requirements;
- review the relevant provisions in other Canadian jurisdictions' laws where legislative officers (or their equivalent) are subject to access and privacy laws; and
- if the government decides to make legislative officers subject to *RTIPPA*, ensure that the necessary legislative amendments properly reflect the role of each legislative officer.

Indigenous access to information and privacy rights

RTIPPA has two provisions involving Crown-Indigenous relations. Both allow for the protection of information provided in confidence by band councils (section 19) and information that, if shared, could harm relations with band councils (section 24).

RTIPPA does not otherwise address the unique principles related to access to information or protection of privacy involving Indigenous peoples. For example, in 1998,

the Assembly of First Nations National Steering Committee first established what later became known as the OCAP® principles related to First Nations data sovereignty. OCAP® stands for ownership, control, access, and possession.[25]

Any changes to *RTIPPA* impacting the specific rights of Indigenous peoples and communities in New Brunswick should only be considered after meaningful consultation to ascertain their needs and expectations surrounding their specific access to information and privacy rights.

Recommendation 27

Ensure that any changes to *RTIPPA* that may impact Indigenous peoples specific access to information and privacy rights reflect the needs and expectations expressed by Indigenous communities and Indigenous right holders.

Privacy impact assessments (PIA)

Unlike New Brunswick's *Personal Health Information Privacy and Access Act* (*PHIPAA*), *RTIPPA* contains no provisions setting out requirements on public bodies to conduct privacy impact assessments. **Privacy impact assessments (PIA) can ensure that privacy considerations are top of mind from the moment a new program, system or service is being developed where the collection, use or disclosure of personal information is anticipated.**

The obligation to conduct PIAs is a growing trend in Canadian jurisdictions, though the provisions found in other provincial and territorial legislation vary in terms of their scope. For example:

- Public bodies subject to PIA requirements: some jurisdictions require all public bodies to conduct PIA's, while others limit this obligation to government departments
- PIA requirements for new or existing programs: some jurisdictions require PIAs for any existing initiative while others require them for only new initiatives
- PIA review: jurisdictions generally require PIAs to be submitted for review and comment, though the entity tasked with this responsibility varies from the Minister responsible for the Act, the head of a public body, or the oversight body (Commissioner/Ombud). In some cases, the Commissioner/Ombud review is required only for matters involving a common or integrated program or service (handling of personal information between more than one entity)

[25] Find more information and resources on OCAP® principles and First Nations data sovereignty from the First Nations Information and Governance Centre at https://fnigc.ca/

While it would be preferable for all public bodies to be required to conduct PIAs, we are also aware that smaller public bodies (municipalities, regional service commissions, etc.) may find it difficult to meet onerous PIA requirements. As such, a phased approach where guidelines, tools and training are readily available to assist public bodies in conducting PIAs may be advisable.

As for the review process for such PIAs, it would be preferable to limit this office to reviewing PIAs involving common or integrated program or services as this would prevent this office from becoming too closely involved with the day-to-day operations of government departments and agencies.

Recommendation 28

Enact PIA requirements in legislation for any new programs, systems or services, that also includes a review mechanism for PIAs. Consideration should be given to implementing the new legislated PIA requirements in phases, beginning with departments and agencies of the Province.

Privacy management programs

Privacy management programs are a framework of policies, procedures, and tools designed to help public bodies comply with privacy laws across their organization. **Robust privacy management programs are recognized as a best practice for privacy risk assessment and compliance both within Canada and internationally.**

While *RTIPPA* does not currently speak to privacy management programs by name, amendments adopted in 2018 include information practices requirements.[26] These set out some of the key components of a privacy management program, including the need to establish information practices to ensure compliance with the *Act* and to protect personal information by making reasonable security arrangements. Public bodies are required to:

- set reasonable retention periods for personal information,
- designate an officer or employee to assist in ensuring compliance and other duties,
- make security arrangements on various issues relating to the handling and protection of personal information,
- periodically test and evaluate the effectiveness of these security arrangements,
- take steps to investigate, document, and notify as required of privacy breaches, and
- follow the Provincial Archivist's record schedules (except for the four public universities).

[26] See *RTIPPA*'s section 48.1 and section 4.2 of its *General Regulation*.

Both British Columbia and Alberta have adopted privacy management program requirements for the public sector, with a view to bolster privacy protection and compliance.

The British Columbia law requires public bodies to develop privacy management programs in line with ministerial directives. Their government has a Privacy Management and Accountability Policy that sets out its scope and policy requirements.

The new law in Alberta also requires public bodies to establish and implement a privacy management program and sets out more details about what this involves as well as public transparency requirements.[27]

The current requirements in *RTIPPA* and its *General Regulation* address many of the key features of a robust privacy management program. There is also room for improvement by adding privacy impact assessment obligations, provisions addressing artificial intelligence and/or automated decision-making, periodic review, assessment, and updating of privacy management programs, and transparency requirements.

Recommendation 29

Amend *RTIPPA* and its *General Regulation* to create requirements for public bodies to adopt and implement comprehensive privacy management programs.

Proactive disclosure

RTIPPA does not require that public bodies proactively disclose information or make information publicly available about the kinds of records held.

Many other Canadian jurisdictions have some level of publication requirements for public bodies about certain aspects of their operations in their respective access laws. Examples of the kinds of information that public bodies are required to publish in other jurisdictions include:

- directories of public bodies and contact information for right to information coordinators;
- descriptions of the public bodies' mandates and functions;
- descriptions or lists of records held by public bodies, including personal information banks;
- manuals, instructions, guidelines, and policy manuals used by public bodies;
- Ministerial expenses;
- briefing materials for new Ministers; and

[27] See Alberta's *Protection of Privacy Act*, s. 25.

- mandate letters.

Examples of Canadian jurisdictions with robust public disclosure requirements include Newfoundland and Labrador, Quebec, Ontario, Manitoba, and the federal government.

Setting up and implementing a publication scheme requires planning and resources. However, **the proactive disclosure of information whenever possible is a positive undertaking that may help reduce routine access to information requests to public bodies.**

Recommendation 30

Enact a publication scheme, having reference to best practices in other jurisdictions including:

- a description of the public body's mandates, functions and programs by branch/division;
- description and list of records under the public body's custody and control, including personal information banks;
- a description of the manuals used to carry out its mandates and functions;
- name and contact information for the public body's head and/or information coordinator.

Voter information

In June 2019, New Brunswick's Chief Electoral Officer published a discussion document entitled Modernizing New Brunswick's Electoral System. Building on a joint statement issued by Federal, Provincial and Territorial Information and Privacy Commissioners in September 2018,[28] the Chief Electoral Officer called for legislative changes to better protect the privacy and security of voter information, namely in relation to political parties.

In March 2025, the Chief Electoral Officer revisited these concerns in an updated report entitled Electoral Data Privacy: A Discussion Document, again calling for legislative and other changes to raise awareness of data privacy challenges and to improve privacy protections in the electoral process. The Chief Electoral Officer consulted the Ombud who supported her recommendations to better protect voter information in the province.

Quebec and British Columbia are currently the only jurisdictions where political parties are subject to access and privacy legislation and oversight through private sector

[28] *Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners: Securing Trust and Privacy in Canada's Electoral Process* (September 2018): https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_180913/.

privacy legislation. Ontario, British Columbia and the federal government have enacted provisions in their respective election laws to require political parties to implement and submit a privacy policy to the Chief Electoral Officer. **This office encourages the Province to continue to explore ways to support greater accountability for registered political parties in their handling of voter information.**

Recommendation 31

Implement legal requirements to ensure:

- registered political parties are subject to privacy requirements;
- an independent body is empowered to verify and enforce privacy compliance;
- individuals have a right to access their personal information in the custody or control of registered political parties.

PART 4 – Recommendations related to the administration of the *Act*

Gaps in consequential amendments and forms

Following the last legislative review of the *Act* in 2018 and the transfer of oversight responsibilities for this *Act* from the Integrity Commissioner to the Ombud in 2019, **this office has noted gaps in consequential amendments resulting in certain forms or legislative and regulatory provisions in this and other Acts that still refer to the Information and Privacy Commissioner.**

A comprehensive scan should be undertaken to correct these inaccuracies in legislation and regulations.

Recommendation 32

Correct any errors in legislation, regulations and forms to ensure that the Ombud is listed as the oversight body under *RTIPPA*.

Public reporting on access to information requests and privacy breaches in the public sector

Finance and Treasury Board has been proactively publishing Annual Reports with statistical information about access to information requests. The current reporting includes core Provincial government departments.

While New Brunswick's current statistical reporting on access to information requests is helpful to give an overview of certain access to information activities and outcomes for core government departments, there is no readily accessible information publicly available for all the other public bodies that are subject to *RTIPPA* (other government agencies, Crown corporations, schools, universities, community colleges, health authorities, municipalities, municipal police forces, and other local government bodies).

Section 16 of Regulation 2010-111 allows the Minister responsible to collect statistical and other information from all public bodies under the *Act* as follows:

> *16(1) The Minister may request from a public body statistical or any other kind of information that, in the opinion of the Minister, is relevant to the proper administration of the Act.*
>
> *16(2) Information submitted to the Minister by a public body shall be submitted*
>
> *(a) in a form and manner acceptable to the Minister, and*
> *(b) by the end of June each year.*

While the Minister can ask public bodies to submit statistical or other information, there is no express requirement for public bodies to do so or to publicly report statistical information on access to information requests or privacy breaches.

Under Manitoba's *Freedom of Information and Protection of Privacy Act*, the responsible Minister is required to report annually on statistical information relating to access requests received by all public bodies:

> *Annual report of responsible minister*
>
> *83(1) The responsible minister shall prepare an annual report and lay a copy of it before the Legislative Assembly if it is in session and, if it is not, within 15 days after the beginning of the next session.*
>
> *Contents of report*
> *83(2) The report under subsection (1) shall include information as to*
> *(a) the number of requests for access that have been made, granted or denied;*
> *(b) the specific provisions of this Act upon which refusals of access have been based;*
> *(c) the number of applications to correct personal information that have been made; and*
> *(d)[repealed] S.M. 2008, c. 40, s. 35;*
> *(e) the fees charged for access to records.*

Having a complete picture of the overall number of requests and how they are being handled would be useful to get a better sense of how the *RTIPPA* is being administered across all public bodies.

Recommendation 33

Amend *RTIPPA* and/or its regulation to require all public bodies to report annually on access to information requests as well as privacy breaches, including the number of reported breaches.

Resources and support for public bodies to meet their access and privacy obligations under *RTIPPA*

This office has a unique perspective as the oversight body for *RTIPPA*. We have worked with many public bodies of all sizes since the law came into force. Our interactions over the years in dealing with access and privacy complaints, public body applications, and privacy breach notifications provide insight into what is working well and where and how public bodies may struggle to meet their obligations.

Public bodies routinely receive broadly worded requests or requests for records that span several years. These can take significant time and resources to process and produce full responses. Applicants may not always trust public body responses and reasons for refusing access, and in some cases, individuals may use access and/or privacy complaints to further their grievances or disputes with public bodies.

Finding the right balance to manage these competing interests can be challenging for all public bodies. It can be particularly so for smaller public bodies, who often do not have the financial resources to have dedicated full-time staff assigned to access and privacy duties.

Adding to this challenge is the fact that New Brunswick is not immune to the rising tide of distrust in public institutions and the effects of misinformation and disinformation, which place bigger demands on governments worldwide. This may make public bodies want to err on the side of caution and be more risk-averse and reluctant to share information out of concern with how it may be interpreted or used. However, it is more critical than ever that public bodies be more open and transparent, not less.

As the challenges facing public bodies are multi-faceted and complex, **government needs to explore how best to support and resource the access to information and privacy infrastructure across all public bodies to ensure that they are able to properly meet their obligations under the *Act*.**

For example, while the Office of the Chief Information Officer in the Department of Finance and Treasury Board serves as a resource to provide guidance and training to RTIPPA coordinators in the core government departments on best practices and interpretation of the *Act*, no such coordinated resource exists for the broader public sector (municipalities, universities, regional health authorities, school districts etc.). While this office can provide general guidance through its reports and other publicly available information, it cannot take on the role of providing advice to those sectors on the day-to-day processing of access to information requests and privacy requirements, given that we may be called upon to examine complaints on these same matters.

Another challenge that needs to be further examined is the capacity to assist public bodies during exceptionally high volumes of requests, usually as a result of a high-profile decision or issue. This office has noted a few examples in recent years where even large and well-resourced provincial government departments were overwhelmed when they received an unexpectedly large influx of access to information requests within a short timeframe. When situations like these occur in smaller public bodies, such as some municipalities, the effects are compounded. Smaller public bodies may not have internal expertise to deal with these exceptional situations, or know to who to ask for assistance. Public bodies would benefit from additional help to assist them in managing these types of challenges.

Recommendation 34

Examine the resources and supports for all public bodies to ensure they can effectively meet their obligations under *RTIPPA*.

Transparency and public debate on proposed changes to *RTIPPA*

Access and privacy rights have been recognized by the courts as being quasi-constitutional in nature and are considered a subset of human rights. As such, *RTIPPA* is a unique piece of legislation that often merits different considerations than other laws.

RTIPPA is a law of general application across the broader public sector in the Province. It recognizes individuals' right to access information about how public bodies make decisions on behalf of the public they serve and to have their privacy protected by public bodies that often hold sensitive personal information.

Given the unique nature of this law, changes that may impact access and privacy rights are of public interest. Special care should be taken by the government and the legislators to ensure that that any changes to the law enhance transparency and accountability of public bodies and bolster, rather than diminish, the access and privacy rights of citizens.

Mandatory reviews of *RTIPPA* are an opportunity to assess what aspects of the law are working well, explore potential changes needed to address new challenges and concerns, identify opportunities for improvement, and to engage and consult with the public and experts in the field.

Given the importance of *RTIPPA* for transparency and accountability in the public sector and its role in building and maintaining trust with the public it serves, the public consultation currently underway at the start of the review is a key opportunity for the government to gather valuable feedback from various perspectives prior to developing legislative amendments.

It would be similarly important for the government to allow for public consultation on any proposed amendments to the law. *RTIPPA* can be a very technical law, which means that its wording needs to be carefully considered to ensure it properly reflects the intent and impact of each provision.

Referring any bills to amend *RTIPPA* to the Legislative Assembly's Standing Committee on Law Amendments would be an effective consultation mechanism. The Standing Committee on Law Amendments can hold public hearings and hear from users and experts who would have the opportunity to weigh in on the exact wording of the proposed changes.

This would further improve the outcome of the overall review of *RTIPPA* and foster a greater sense of openness and trust between the government and the public.

Recommendation 35

Refer any proposed amendments to *RTIPPA* to the Legislative Assembly's Standing Committee on Law Amendments for review and public hearings, in recognition of the quasi-constitutional nature of this legislation.

APPENDIX 1 – Summary of recommendations

PART 1 - Recommendations related to *RTIPPA*'s current provisions	
Recommendation 1	Amend the definition of "government body" in section 1 to expand it to: • bodies whose majority of members, officers, and/or directors are appointed by an Act, a minister or the Lieutenant-Governor in Council; and • those the government owns or in which it has a controlling interest.
Recommendation 2	Amend the definition of "personal information" in section 1 to include biometric information.
Recommendation 3	Amend section 1 to define terms such as artificial intelligence, generative artificial intelligence, and automated decision-making.
Recommendation 4	Amend the purpose clause in section 2 to reference democratic and transparency principles behind access to information and reinforce the importance of protecting privacy.
Recommendation 5	Repeal the paragraph 4(b) exclusion.
Recommendation 6	Amend *RTIPPA* by adding a Schedule to include a list of all legislative provisions that prevail over *RTIPPA* and specify that the contents of the said Schedule be subject to any review of *RTIPPA* initiated under section 86.1.
Recommendation 7	Assess the impact of the extended timelines on public bodies' ability to provide timely and fulsome responses to access to information requests and reconsider the timelines to align with the standards set out in most other Canadian jurisdictions.
Recommendation 8	Maintain the oversight role of the Ombud on requests to disregard an access to information request under *RTIPPA*.
Recommendation 9	Amend paragraph 15(a) to ensure the English and French versions have the same meaning and effect.
Recommendation 10	Amend *RTIPPA* to improve the processes for disregarding access to information requests, namely: • a requirement to notify applicants when an access request has been set aside; • time limits to file and render decisions for applications to disregard;

	• clarifying the requirement to process access to information requests pending a decision on disregarding the request; and allowing the applicant to appeal to the courts when an access request is disregarded by a public body.
Recommendation 11	Amend *RTIPPA* to allow for a broader disclosure of Cabinet records.
Recommendation 12	Remove the requirement in subsection 17(2) for Executive Council approval for disclosure after 10 years.
Recommendation 13	Amend section 21 to include factors to consider in determining when the disclosure of personal information would and would not be an unreasonable invasion of privacy.
Recommendation 14	Amend section 22 to create a three-part harms-based test.
Recommendation 15	Amend paragraph 26(2)(a) to reduce the blanket protection for all records related to advice to public bodies to make it consistent with the protection afforded to Cabinet records under section 17.
Recommendation 16	Amend *RTIPPA* by: • removing the exception for Executive Council confidences and solicitor-client privilege found in subsection 70(1) • specifying that production of information or a record to the Ombud for review does not constitute a waiver of legal privilege • allowing the Ombud to apply to the courts for an order for the production of records.
PART 2 – Recommendations related to *RTIPPA*'s General Regulation	
Recommendation 17	Amend the definition of "privacy breach" in section 4.2 to include circumstances where personal information has been lost or stolen.
Recommendation 18	Amend the *General Regulation* to require notifying the Ombud of referrals and appeals to the court and that court decisions be provided to the Ombud.
Recommendation 19	Amend the *General Regulation* to include a process for appeals filed by the Ombud, and add a prescribed form for appeals initiated by the Ombud.
PART 3 - Recommendations related to other public policy issues	
Recommendation 20	Enact a requirement for public bodies to consult with the Ombud on draft laws that could have implications for access to information or protection of privacy.

Recommendation 21	Amend *RTIPPA* to create a statutory right for the Ombud to intervene in court referrals and appeals.
Recommendation 22	Adopt a hybrid model, maintaining the Ombud's recommendation powers and instituting a requirement for public bodies to obtain a court order to set aside recommendations made by the Ombud on access to information or privacy matters.
Recommendation 23	Amend *RTIPPA* to provide a legal framework to define: • the rights and standards related to the handling of personal information involved in automated decision-making schemes; appropriate safeguards and rights for New Brunswickers in the creation and use of automated decision-making schemes by public bodies
Recommendation 24	Create a legislated duty requiring public bodies to document matters related to key actions and decisions, along with oversight and enforcement provisions.
Recommendation 25	Enact a general public interest override clause for all discretionary exceptions to disclosure and include a list of factors to consider in assessing public interest disclosure.
Recommendation 26	Ensure that the following steps be taken before deciding on the expansion of *RTIPPA* to legislative officers: • consult with each legislative officer to identify and explore any mandate-specific concerns they may have, including existing statutory confidentiality and public disclosure requirements; • review the relevant provisions in other Canadian jurisdictions' laws where legislative officers (or their equivalent) are subject to access and privacy laws; and if the government decides to make legislative officers subject to *RTIPPA*, ensure that the necessary legislative amendments properly reflect the role of each legislative officer.
Recommendation 27	Ensure that any changes to *RTIPPA* related to specific access to information and privacy rights reflect the needs and expectations expressed by Indigenous communities and Indigenous right holders.
Recommendation 28	Enact PIA requirements in legislation for any new programs, systems or services, that also includes a review mechanism for PIAs. Consideration should be given to implementing the

	new legislated PIA requirements in phases, beginning with departments and agencies of the Province.
Recommendation 29	Amend *RTIPPA* and its *General Regulation* to create requirements for public bodies to adopt and implement comprehensive privacy management programs.
Recommendation 30	Enact a publication scheme, having reference to best practices in other jurisdictions including: • a description of the public body's mandates, functions and programs by branch/division; • description and list of records under the public body's custody and control, including personal information banks; • a description of the manuals used to carry out its mandates and functions; name and contact information for the public body's head and/or information coordinator.
Recommendation 31	Implement legal requirements to ensure: • registered political parties are subject to privacy requirements; • an independent body is empowered to verify and enforce privacy compliance; individuals have a right to access their personal information in the custody or control of registered political parties.
PART 4 – Recommendations related to the administration of the *Act*	
Recommendation 32	Correct any errors in legislation, regulations and forms to ensure that the Ombud is listed as the oversight body under *RTIPPA*.
Recommendation 33	Amend *RTIPPA* and/or its regulation to require all public bodies to report annually on access to information requests as well as privacy breaches, including the number of reported breaches.
Recommendation 34	Examine the resources and supports for all public bodies to ensure they can effectively meet their obligations under *RTIPPA*.
Recommendation 35	Refer any proposed amendments to *RTIPPA* to the Legislative Assembly's Standing Committee on Law Amendments for review and public hearings, in recognition of the quasi-constitutional nature of this legislation.

ombud
NEW BRUNSWICK • NOUVEAU-BRUNSWICK

ombudnb.ca

Tel • Tél.: (506) 453-2789 | 1-888-465-1100

Fax • Télécop.: (506) 453-5599

Email • Courriel: ombud@gnb.ca

PO Box 6000 • CP 6000
Fredericton NB E3B 5H1
Canada