



**Submission by the Office of the Information and Privacy Commissioner for Nova Scotia to the Nova Scotia Government Working Group on the review of the *Freedom of Information and Protection of Privacy Act*, related legislation, and regulations**

**January 31, 2024**

**Contents**

Contents..... 1

Glossary ..... 3

Commissioner’s message ..... 4

Introduction ..... 6

    A preliminary matter: transparency of the Legislative Review..... 7

    The need for improved leadership and a cultural shift ..... 7

    The need for sufficient resources ..... 8

    What is working ..... 9

    Structure of the OIPC’s submission ..... 9

**A. Organization and coverage ..... 10**

    Mutatis mutandis..... 10

    Extending coverage to political parties..... 10

**B. Modernizing access rights..... 11**

    Definitions ..... 11

        (i) Definition of “prosecution” ..... 11

        (ii) Definition of “exercise of prosecutorial discretion” ..... 12

    Solicitor-client privilege..... 12

        (i) Production of records for review by the Commissioner ..... 12

        (ii) Settlement privilege..... 13

    Time extension requests..... 14

        (i) The possibility for multiple time extensions ..... 14

        (ii) The need for time extension requests ..... 15

        (iii) Additional time extension powers are needed ..... 17

    Deemed refusal due to sign-off..... 18

    Notices to third parties..... 19

    Anonymity of applicants ..... 21

    Limited and specific exemptions: non-responsive ..... 22

    Indigenous issues ..... 24

    Compassionate disclosure..... 25

**C. Modernizing privacy rights ..... 26**

    Definition of “use of personal information” ..... 26

Young people’s privacy.....	27
Who can act for a child and young people .....	27
<i>PIIDPA</i> .....	28
Emerging issues and technologies .....	29
(i) Automated decision-making, artificial intelligence, and generative artificial intelligence.....	29
(ii) Biometrics.....	31
(iii) Data linking.....	32
<b>D. Improving oversight.....</b>	<b>33</b>
Independence of the OIPC: funding.....	33
Reasons for rejecting the Commissioner’s recommendation(s).....	34
Role of access and privacy administrators .....	36
Powers of the Commissioner .....	39
Other minor improvements.....	39
Appendix A - List of recommendations .....	40
Appendix B - Suggested readings .....	44

## Glossary

**Access:** Access to information

**Access and privacy laws:** Four of the laws in Nova Scotia related to access and privacy: *FOIPOP*, *MGA*, *PRO*, and *PIIDPA*

**Access and privacy regime:** The systems, culture, and processes associated with the access and privacy laws in Nova Scotia

**FOIPOP:** The *Freedom of Information and Protection of Privacy Act*

**Government:** The Nova Scotia Government

**IPC:** Information and Privacy Commissioner

**IAP Services:** Information Access and Privacy Services for the Nova Scotia Government

**Internal Working Group:** The working group made up solely of internal Nova Scotia Government employees to review Nova Scotia's access and privacy laws for the Legislative Review

**Legislative Review:** The Nova Scotia Government's mandated review of Nova Scotia's entire access and privacy legislative framework

**MGA:** *Part XX of the Municipal Government Act*

**OIPC:** The Office of the Information and Privacy Commissioner for Nova Scotia

**PHIA:** The *Personal Health Information Act*

**PIIDPA:** The *Personal Information International Disclosure Protection Act*

**PRO:** The *Privacy Review Officer Act*

**Public body/public bodies:** All entities covered by *FOIPOP*, *PRO*, and *PIIDPA* such as government departments, universities, regional centres for education, health authorities, agencies, boards and commissions as well as all entities covered by the *MGA*, such as municipalities and municipal bodies, municipal police, and transit authorities

**S.:** Section of a legislative Act

**2017 Special Report:** The IPC's 2017 *Accountability for the Digital Age, Modernizing Nova Scotia's Access & Privacy Laws Report*

**2021-2022 Annual Report:** The 2021-2022 Annual Report of the Office of the Information and Privacy Commissioner for Nova Scotia

## Commissioner's message

In 2021, the Nova Scotia Government gave the Minister of Justice a [mandate](#) to amend [FOIPOP](#) so that the Information and Privacy Commissioner<sup>1</sup> would be given order-making power. In 2023, the Government [announced](#) that an Internal Working Group had been struck to review the entire access and privacy legislative framework in Nova Scotia. Given the array of access and privacy laws in Nova Scotia and given that they have not been reviewed in a considerable amount of time, this Legislative Review is enthusiastically welcomed. I also welcome the Internal Working Group's commitment to continually engage with my office throughout its review.

The Legislative Review also presents a perfect opportunity for the Nova Scotia Government to evaluate issues that exist in addition to problems with the laws. Like many other provinces and territories, the problems plaguing access to information and protection of privacy in Nova Scotia are not solely legislative ones. There are two main others: cultural and leadership practices that disregard the public's presumptive right to public body information, and insufficient resources allocated to the access and privacy regime. This submission addresses these problems alongside its recommendations for changes to the laws.

The sentiment that strong access and privacy laws are not necessarily enough to ensure fulfillment of peoples' access and privacy rights is not new. When the existing *FOIPOP* was being debated in the Legislative Assembly, prior to its enactment, the then Minister of Justice [said](#), "...the current Act failed to create openness in government because access to information is more than legislation, it is also a program and a commitment." He argued that one of the problems with past implementation was, "...that the previous government did not create a climate of openness, in my opinion. It did not say to its staff that it is more prudent to release the information than to withhold it."

It is unfortunate that 30 years later, this problem is still widespread. In the reviews that my office conducts, we frequently see decisions that disregard the public's presumptive right to all public body information, subject only to the limited and specific exemptions spelled out in the laws. My office was created to uphold this right. But when we are so underfunded that we've had a four-year backlog since 2020 (and an ongoing backlog since 2013), our ability to uphold the laws' goals is significantly hindered.

Our ability is further hindered by many public bodies' approaches to dealing with my office when we conduct reviews of their decisions to withhold information. My office puts a substantial amount of time and effort into helping public bodies understand their legal obligations and explaining to them how and why the laws mean they can or cannot

---

<sup>1</sup> Effective September 2015, the OIPC began referring to the *FOIPOP* Review Office as the Office of the Information and Privacy Commissioner and the Review Officer and Privacy Review Officer as the Information and Privacy Commissioner. I will use those terms throughout this submission. No legislative change was made and so *FOIPOP*, *PRO*, and the *MGA* use the old titles of Review Officer and Privacy Review Officer. See Recommendation 23 of the [2017 Special Report](#) for the IPC's recommendation to amend the language in the access and privacy laws.

withhold information. This effort is frequently disproportionate to the time and effort put in by public bodies, who, I note, are usually better resourced and better funded than my office. Many times, it seems as though public bodies' engagement with us is more performative than meaningful. I say this because public bodies continue to regularly advance arguments that have long been rejected. They do not address, consider, or rebut our comprehensive analyses, opinions, and recommendations. This results in applicants not receiving transparent or justifiable reasons for why public bodies are withholding information. This is frustrating for me and my staff, but the people who lose out the most in this situation are Nova Scotians.

When explaining why the Act preceding the current *FOIPOP* needed updating, the then Minister of Justice also [said](#):

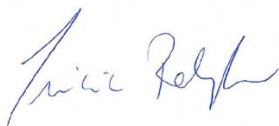
Let me say now, this government would rather be criticized for something contained in information it releases than be criticized for not releasing the information. We can move forward from criticisms for mistakes, but no government can advance its program under a cloud of suspicion.

This Legislative Review presents public bodies with an opportunity to approach their obligations as the then Minister of Justice intended. It also presents the Nova Scotia Government with the opportunity to once again be a leader in protecting and fostering access and privacy rights, as it was when it was the first jurisdiction in Canada to enact freedom of information legislation. To get there, genuine leadership at the highest level is needed. I sincerely hope for and encourage the Nova Scotia Government to make real changes to both Nova Scotia's laws and to the entire access and privacy regime. It is time for public bodies to not simply talk the talk but to truly fulfill their access and privacy obligations.

Many of the recommendations in this submission are similar to and modified from ones previously made by my counterparts across the country. I would like to acknowledge their work and thank them for this submission's reliance on their previous efforts to improve the access and privacy regimes of this country.

I would also like to thank Carmen Stuart, OIPC's Executive Director, for helping to draft this submission, and the many others in my office who contributed to its development. In the face of the many obstacles that frustrate the OIPC's work, their commitment to ensuring that the laws are implemented for their intended purpose – to facilitate democracy – is truly commendable.

Respectfully submitted,



Tricia Ralph  
Information and Privacy Commissioner for Nova Scotia

## Introduction

In 2021, the Nova Scotia Government gave the Minister of Justice a [mandate](#) to amend [FOIPOP](#). In September 2023, an Internal Working Group (made up solely of Nova Scotia Government officials) was formed to conduct a review of all of Nova Scotia’s access and privacy laws.<sup>2</sup>

Nova Scotia was once the leader of access and privacy laws in this country by being the first jurisdiction in Canada to enact a freedom of information law in 1977. In 1994, the *FOIPOP* that exists today replaced the 1977 version. Several additional pieces of legislation were added over the years<sup>3</sup> but no substantial amendments have been made to *FOIPOP* in 30 years.

The access and privacy world has changed exponentially in 30 years. All around Nova Scotia, provinces and territories have acted to incrementally modernize their laws in response to these developments. But Nova Scotia has not. This leaves Nova Scotians with fewer protections and less effective access and privacy rules than citizens in other Canadian jurisdictions.

This Legislative Review is enthusiastically welcomed, as at this point, there is no question that Nova Scotia is falling behind on both a national and international scale. Nova Scotians deserve better, and now is the time to correct the widening gap with respect to Nova Scotia’s access and privacy laws.

But it is not just access and privacy laws that need to be addressed. Nova Scotia’s entire access and privacy regime is so outdated that it also needs a fulsome overhaul.

Access and privacy rights are critical components of a healthy democracy. Like many other provinces and territories, the problems plaguing access to information and protection of privacy rights in Nova Scotia are not solely legislative ones. These rights are fulfilled not only through robust access and privacy laws but also through the proper implementation of them.

The sentiment that strong access and privacy laws are not necessarily enough to ensure fulfillment of peoples’ access and privacy rights is not new. When the existing *FOIPOP* was being debated in the Legislative Assembly, prior to its enactment, the then Minister of Justice [said](#), “...implementation of the new Act is almost as important as the bill itself.” The Minister expressed concern that additional resources were not available for implementation. He noted that “...the current Act failed to create openness in government

---

<sup>2</sup> The Legislative Review does not include a review of [PHIA](#), however its terms of reference state that the review will consider changes to *PHIA* where there is a direct overlap with any changes made to *FOIPOP*. The OIPC agrees that any amendments resulting from this Legislative Review should be considered for *PHIA* as well.

<sup>3</sup> The *Municipal Government Act*, SNS 1998, c 18, ([MGA](#)) in 1999; the *Personal Information International Disclosure Protection Act*, SNS 2006, c 3, ([PIIDPA](#)) in 2006; the *Privacy Review Officer Act*, SNS 2008, c 42, ([PRO](#)) in 2009; and the *Personal Health Information Act*, SNS 2010, c 41, (*PHIA*) in 2013.

because access to information is more than legislation, it is also a program and a commitment.” He argued that one of the problems with past implementation was, “...that the previous government did not create a climate of openness, in my opinion. It did not say to its staff that it is more prudent to release the information than to withhold it.”

In the OIPC’s view, these problems with implementation remain today: leadership that does not clearly identify disclosure expectations, and insufficient resources allocated to the access and privacy regime. To ensure any amendments to Nova Scotia’s access and privacy laws arising from this Legislative Review are not overshadowed and made hollow by insufficient implementation efforts, this submission recommends actions not only to update the statutory framework, but also to address areas for improvement in leadership and resourcing.

### ***A preliminary matter: transparency of the Legislative Review***

Any review of access and privacy laws will undoubtedly draw feedback and suggestions from all different types of stakeholders with varying interests. Some stakeholders will likely encourage changes to the laws that are based on incorrect or rebuttable conclusions. Some feedback will likely suggest that access requirements are too broad and too onerous to fulfill. The Internal Working Group may hear that responding to access requests takes too much time, taxes an already overburdened system, and interferes too much with the operations of public bodies. The OIPC has certainly heard these concerns many times.

The [Terms of Reference](#) for the Legislative Review do not indicate that stakeholder submissions will be made public. If stakeholder submissions are kept confidential, then the OIPC (who is best situated to provide explanation and context for any incorrect stakeholder assertions), and other stakeholders will lose the ability to provide context to the submissions of others.

The OIPC believes that any amendments to Nova Scotia’s access and privacy laws will benefit when the submissions of those who participate in the Legislative Review are subject to scrutiny from all, so that any ungrounded assertions may be addressed. It is for this reason that the OIPC encourages the Internal Working Group to make public all submissions (subject to any privacy concerns) as well as its findings and recommendations, so that there is an opportunity to respond.

### ***The need for improved leadership and a cultural shift***

Access and privacy laws give public bodies considerable discretion to not disclose requested information even if they are allowed to. The OIPC rarely sees cases where a public body’s exercise of discretion results in disclosure when the laws allow for but do not mandate it.

A fair number of the reviews the OIPC receives would likely not see a different outcome if Nova Scotia’s access and privacy laws were different. In many cases, the laws actually work, but the problem is the public body’s failure to interpret and implement them appropriately.



Because the IPC only has recommendation and not order-making power, public bodies can simply choose to reject the Commissioner's recommendation(s) with little recourse, as few applicants can afford to challenge their decisions in the Supreme Court of Nova Scotia.

While an amendment to give the Commissioner order-making power or to put a reverse-onus on public bodies when they do not wish to follow the Commissioner's recommendations will likely alleviate much of this problem, it needs to be accompanied by a significant cultural shift in public bodies' approach to complying with the laws. A significant cultural shift requires strong leadership.

Robust leadership is needed to initiate a culture shift towards truly embracing the purposes of Nova Scotia's access and privacy laws: being fully accountable to the public, providing disclosure of all government information except in limited and specific circumstances, and protecting privacy.

### *The need for sufficient resources*

For years the access and privacy regime in Nova Scotia has been woefully under-resourced both at the OIPC and at many public bodies.

The OIPC's calls for adequate staff have not resulted in enough staff to effectively run the office. The OIPC has a four-year backlog for hearing complaints. There is no denying that this is unacceptable. Information that is outdated often becomes irrelevant when more than four years have passed before the OIPC can conduct its independent review of public bodies' decisions to withhold information.

From the OIPC's vantage point, many public bodies are under-resourced as well. They frequently take and request the OIPC's permission for time extensions that a body of their size should be able to handle without the need for one. Many times, they simply do not reply in time and so are deemed to have refused to disclose the records to an applicant. Evidence of under-resourcing is particularly apparent to the OIPC during the OIPC review process. Public bodies frequently provide bare bones, pro forma rationales for withholding information that reject years of decisions from the OIPC, other IPC offices from across the country, and the Supreme Court of Nova Scotia. They rarely provide justifiable reasons for rejecting the OIPC's expertise. This significantly frustrates the purposes of Nova Scotia's access and privacy laws. It hinders the public's ability to hold public bodies fully accountable and it jeopardizes the democratic process. It also indicates either insufficient resources to research the law and substantiate decisions or a lack of clarity from leadership about disclosure expectations. Either way, it also further strains the OIPC's limited resources because the OIPC needs to spend so much time explaining the law to public bodies that should well know it.

Most of the recommendations in this submission will require increased resources in terms of both staffing and funding. Without adequate resourcing, many amendments resulting from this Legislative Review will be rendered meaningless. For this reason, the OIPC

encourages the Internal Working Group to not only recommend legislative changes but also financial ones. This is in keeping with Recommendation 24 of the [2017 Special Report](#).

### ***What is working***

Before getting into the areas where Nova Scotia's access and privacy laws could use improvement, it is important to note that there are many aspects of the laws that work well. One of those is the strength of the purpose clauses.

The purpose clauses in Nova Scotia's access and privacy laws have been recognized by the Nova Scotia Court of Appeal as being intended to give the public greater access to information than those in all other Canadian provinces and territories.<sup>4</sup> They are arguably the most robust and progressive in Canada and they work well. The purpose clauses are the envy of other jurisdictions. The OIPC encourages the Internal Working Group not to recommend changes to the purpose clauses that currently exist.

The OIPC is also concerned that if changes are made from this Legislative Review, they may be ones that erode some of the benefits of the existing access and privacy laws. For this reason, the OIPC encourages the Internal Working Group to not recommend further limits on disclosure such as more exemptions, more exclusions, and more time allotments.

### ***Structure of the OIPC's submission***

The OIPC has previously released two main documents setting out its recommendations for amendments to Nova Scotia's access and privacy laws. The *2017 Special Report* outlined in detail many recommendations for modernization. Updates to these recommendations were set out in the OIPC's [2021-2022 Annual Report](#). The OIPC has largely not repeated the recommendations in those two documents in this submission, but it is important that they be read in tandem with it. Many of the OIPC's most crucial recommendations are set out in those two documents.

In this submission, the OIPC will focus on shedding light on how Nova Scotia's access and privacy laws are working, or more accurately, how they are not working. It also provides further recommendations to improve Nova Scotia's access and privacy regime.

For consistency, this submission is organized into the same four parts as the OIPC's last two published calls for legislated amendments. They are (a) organization and coverage, (b) modernizing access rights, (c) modernizing privacy rights, and (d) improving oversight.

---

<sup>4</sup> *O'Connor v. Nova Scotia*, [2001 NSCA 132 \(CanLII\)](#), at paras. 54-57.

## A. Organization and coverage

Nova Scotia has a confusing array of access and privacy laws. More modern laws typically combine all access and privacy laws into one single law (with the exception of health information and privacy laws). Recommendation 1 of the [2017 Special Report](#) and the [2021-2022 Annual Report](#) was to combine these laws into one law (except for [PHIA](#)).

This array of laws causes many issues. It can be confusing for applicants. Not all the laws provide for independent oversight. There are inconsistencies across the laws. It frankly just doesn't make sense. Rather than get into specifics about which Acts have which need for change, this submission simply refers to "access and privacy laws" to mean that all the recommendations in this submission should be viewed from the lens of ensuring all are addressed in one resulting piece of legislation (with the exception of [PHIA](#)). That being said, there is a significant inconsistency that the OIPC has recently realized and so it is included here. It is the issue of the *mutatis mutandis* provision in s. 3 of [PRO](#).

### *Mutatis mutandis*

Neither [FOIPOP](#) nor the [MGA](#) set out the IPC's powers in terms of privacy oversight. In an effort to address this in 2009, [PRO](#) was created to give the Commissioner privacy oversight. Instead of recreating all of the Commissioner's powers when conducting a review already set out in [FOIPOP](#), [PRO](#) says that sections 34-41 of [FOIPOP](#) applies to it. The problem is that there are some important powers in [FOIPOP](#) that should also apply to [PRO](#) but do not because they fall outside of sections 34-41. For example, sections 34-41 do not include the sections of [FOIPOP](#) that give the courts power to review a privacy complaint or for someone to act on behalf of another person when filing a privacy complaint.

**Recommendation 1: Ensure that the privacy provisions in [PRO](#) are combined with all other Nova Scotia access and privacy laws into one complete Act.**

### *Extending coverage to political parties*

Access and privacy laws in Nova Scotia only apply to public bodies. This means that a variety of entities, such as the offices of Members of the Legislative Assembly (MLA) and officers of the legislature are not subject to Nova Scotia's access and privacy laws. Recommendation 2 of the [2017 Special Report](#) recommended that access and privacy laws be extended to include MLA offices and officers of the legislature when dealing with personal information.

Since that time, it has become clear that another major type of organization should also be subject to access and privacy laws – political parties.

Not having political parties be required to follow access and privacy laws is problematic. This is because political parties typically gather vast amounts of personal information to target individuals, in specific ways, for political gain. In recent years, it has been made public that there has even been misuse of personal information for political gain. An

example of this is Cambridge Analytica’s manipulation of Facebook data to profile American voters.

In 2018, Canada’s Privacy Commissioners passed a joint resolution titled [Securing Trust and Privacy in Canada’s Electoral Process](#). This resolution called on governments to pass legislation:

1. Requiring political parties to comply with globally recognized privacy principles;
2. Empowering an independent body to verify and enforce privacy compliance by political parties through, among other means, investigation of individual complaints; and,
3. Ensuring that Canadians have a right to access their personal information in the custody or control of political parties.

Despite this, in Nova Scotia and in most of the rest of Canada, political parties continue to not be required to follow access and privacy laws. The exception to this is some jurisdictions with private sector legislation, namely British Columbia,<sup>5</sup> and [Quebec](#).

In a democracy, it is typical for political parties to collect personal information about voters. However, this should not be a free-for-all. Individuals should know what personal information is being collected about them and what political parties are doing with that information. Political parties should be required to inform individuals of any privacy breaches and individuals should be able to complain to an independent oversight body about their privacy practices. While it may be that political parties should not be considered as public bodies for all the purposes of access and privacy laws, they should certainly be in terms of their handling of personal information, including oversight.

**Recommendation 2: Amend Nova Scotia’s access and privacy laws to make political parties subject to the personal information and oversight rules set out in them.**

## **B. Modernizing access rights**

### ***Definitions***

Applying the law is all about interpretation, however some things should not be open to interpretation and would benefit from clearer language in the laws.

#### **(i) Definition of “prosecution”**

There are certain times in Nova Scotia’s access and privacy laws where categories of records are excluded, meaning the laws don’t apply to them and applicants cannot get them. One of those categories is records relating to an incomplete prosecution.

---

<sup>5</sup> *Personal Information Protection Act*, [SBC 2003, c 63](#), s. 3(1). For more information see BC’s [Investigation Report P19-01: Full Disclosure: Political parties, campaign data, and voter consent](#).

Nova Scotia's access and privacy laws do not include a definition of the term "prosecution". The OIPC has experience where police forces apply the exclusion for records relating to a prosecution when the records do not relate to any active investigation. They withhold records in any investigation on the basis that the investigation could lead to charges being laid and if charges are laid, the matter could proceed to prosecution.

The OIPC does not interpret this to be the intention of the exclusion. The OIPC believes a prosecution needs to be started for this exclusion to apply. It is not triggered simply because charges in the future are a possibility. Rather, only those records that are related to an active prosecution should be considered under this exclusion. The law enforcement provisions of the access and privacy laws provide protection of law enforcement information that is not yet subject to a prosecution.

**Recommendation 3: Amend Nova Scotia's access and privacy laws to include a definition of the term "prosecution" and clarify when it starts.**

**(ii) Definition of "exercise of prosecutorial discretion"**

Access and privacy laws allow public bodies to withhold information that could reasonably be expected to reveal any information relating to or used in the exercise of prosecutorial discretion. However, the phrase "exercise of prosecutorial discretion" is not defined.

Unlike Nova Scotia, Schedule 1 of British Columbia's [Freedom of Information and Protection of Privacy Act \(FIPPA\)](#) provides a definition of the phrase "exercise of prosecutorial discretion". British Columbia's definition was originally followed in the Nova Scotia case of [Cummings v. Nova Scotia \(Public Prosecution Service\)](#). Subsequently, in [Nova Scotia \(Public Prosecution Service\) v. FitzGerald Estate](#), the Nova Scotia Court of Appeal thoroughly canvassed the meaning of "prosecutorial discretion" and relied on the Supreme Court of Canada decision in [Krieger v. Law Society of Alberta](#) to set out a number of principles regarding the phrase.<sup>6</sup> These principles are lengthy and fairly complex. It would be helpful for them to be codified in Nova Scotia's access and privacy laws.

**Recommendation 4: Amend Nova Scotia's access and privacy laws to include a definition of the phrase "exercise of prosecutorial discretion".**

***Solicitor-client privilege***

**(i) Production of records for review by the Commissioner**

Over the years, courts have reduced Commissioners' authority to investigate complaints when a public body claims records are subject to solicitor-client privilege. More specifically, courts have largely said that except in certain circumstances, Information and Privacy Commissioners are not entitled to require production of records to which the solicitor-client exemption has been applied by a public body.

---

<sup>6</sup> NS Review Report FI-11-72 (Amended), *Public Prosecution Service (Re)*, [2015 NSOIPC 10 \(CanLII\)](#) gives an excellent summary of the evolution of the law in this area.

This has not been an issue in Nova Scotia, but given the case law coming out elsewhere, it should be addressed in any amendments to Nova Scotia’s access and privacy laws. In Recommendation 23 of the [2017 Special Report](#) and the [2021-2022 Annual Report](#), the OIPC put forward its position that it should have the power to compel production of records to which the solicitor-client exemption has been applied by a public body. However, given the importance of this issue, and some recent developments since then, the OIPC is reiterating its recommendation in this submission.

This issue has a complex history with a complex set of court decisions, making it difficult to paint the full picture for the purpose of this submission. There continue to be developments in this area. For example, in 2015, Newfoundland and Labrador incorporated a provision that was intended to make clear that the Commissioner has the right to compel production of any record for which solicitor-client privilege has been claimed into its [Access to Information and Protection of Privacy Act \(ATIPPA\)](#). Despite this, in the 2023 case of [Newfoundland and Labrador \(Information and Privacy Commissioner\) v Newfoundland and Labrador \(Justice and Public Safety\)](#), the Court of Appeal of Newfoundland and Labrador found that the language used was insufficiently clear, explicit, and unequivocal to override solicitor-client privilege.

**Recommendation 5: Amend Nova Scotia’s access and privacy laws to ensure there is clear, explicit, and unequivocal language that the Commissioner can require production and examination of all records to which the solicitor-client privilege exemption has been applied by a public body.**

#### **(ii) Settlement privilege**

At times, public bodies may enter into a settlement agreement, covered by settlement privilege, to settle a court or other matter. What this means for a typical legal case is that a document covered by settlement privilege cannot then be used in any other way. But what happens when someone asks for such a record when one of the parties is a public body and so is subject to Nova Scotia’s access and privacy laws? When such a record is requested, the OIPC has seen public bodies withhold it based on the common-law principle of settlement privilege. But there is no exemption in Nova Scotia’s access and privacy laws that explicitly says public bodies can withhold records under settlement privilege. So, public bodies say that this common-law principle stands regardless of access and privacy laws – that it exists as a “free-standing” exemption. In [NS Review Report 16-12](#), the Commissioner rejected this argument. She said that Nova Scotia’s laws provide a comprehensive code of exemptions and do not permit the addition of a free-standing exemption based on the common-law principle of settlement privilege. She said that if an exemption in relation to this information exists, it must be found within the terms of Nova Scotia’s access and privacy laws.

Other public bodies have argued that the exemption for solicitor-client privilege encompasses settlement privilege. In [Daniels v. Wolfville \(Town\)](#), Justice Gatchalian, J. said that “solicitor-client privilege” and “settlement privilege” are distinct concepts. In other words, the existing solicitor-client privilege exemption does not include the concept of settlement privilege. What this means is that because there is not an exemption that

explicitly refers to settlement privilege in Nova Scotia, settlement privilege cannot be used to exempt records or information. However, there has been a trend across the country to read settlement privilege into the definition of solicitor-client privilege.<sup>7</sup> This creates a confusing situation for Nova Scotia and so should be addressed in this Legislative Review.

**Recommendation 6: Amend Nova Scotia’s access and privacy laws to make clear that settlement privilege is not an exemption under which public bodies can withhold information.**

### *Time extension requests*

Nova Scotia’s access and privacy laws require public bodies to respond to access requests within 30 days unless a time extension is taken. Public bodies are allowed to extend the time to respond for an additional 30 days so long as they meet criteria set out in the law (such as the applicant does not give enough detail to help the public body identify the requested record). Before those 60 days are up, public bodies can also ask the OIPC to grant them additional time extensions, which could be for any amount of time.

#### **(i) The possibility for multiple time extensions**

In 2023, the OIPC was taken to court by an applicant who disagreed with its interpretation of the time extension provisions. Nova Scotia’s access and privacy laws say that a public body can take a 30-day time extension on its own accord so long as it meets criteria set out in the law. It also says that the OIPC can permit longer time extensions when public bodies meet the criteria in the law.

What happened in the court case was that after a public body had taken its initial time extension on its own initiative, it requested permission from the OIPC for a second time extension. The OIPC granted this request. The applicant argued that the legislation only gave “either/or” options, meaning public bodies can either take their own time extension or they can ask for permission for a longer time extension from the OIPC, but public bodies cannot do both. The OIPC had always interpreted the access and privacy laws to mean that public bodies can take their own time extension and can also seek permission for additional ones from the OIPC. The applicant disagreed and so filed a judicial review application with the Supreme Court of Nova Scotia.

The applicant’s judicial review was dismissed. In [\*Donham v. Nova Scotia \(Information and Privacy Commissioner\)\*](#), the Supreme Court of Nova Scotia said that the OIPC’s decision to grant a second longer period time extension after the public body had already taken its initial 30-day time extension was, “...justifiable, transparent and intelligible.” This result was welcomed but the court case did have an impact on the OIPC’s limited resources – both staff hours preparing a response and financially.<sup>8</sup> While the court decision has resolved this question, it would be beneficial to make it clear in the wording of access and privacy laws. Section 10 of British Columbia’s [\*FIPPA\*](#) is a good example.

---

<sup>7</sup> See for example, *Richmond (City) v. Campbell*, [2017 BCSC 331 \(CanLII\)](#).

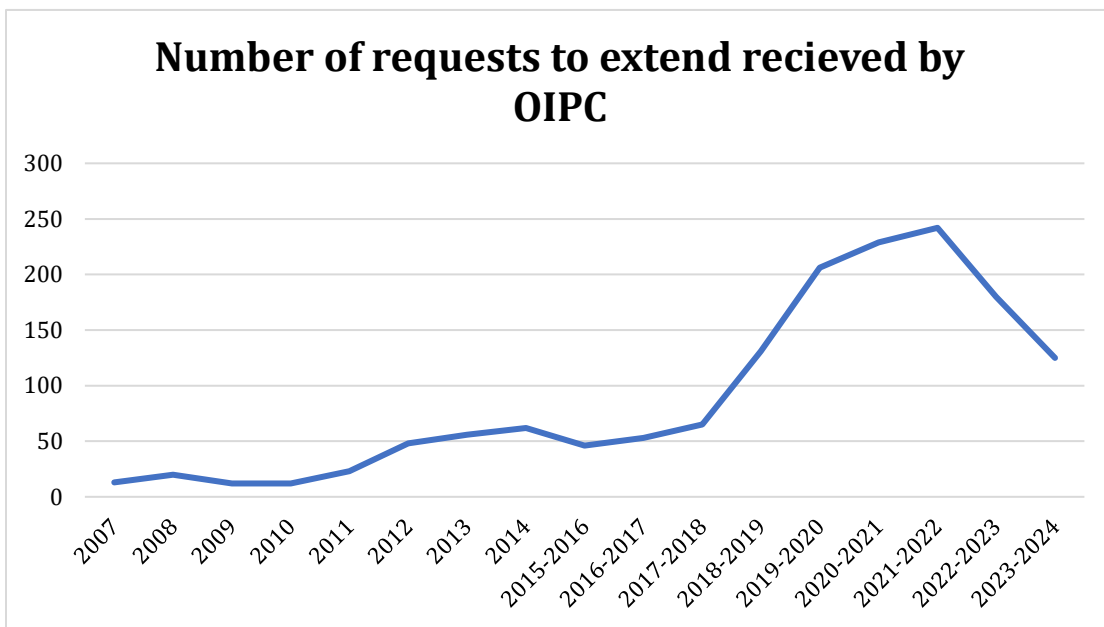
<sup>8</sup> See page 15 of the OIPC’s [2022-2023 Annual Report](#) for more information about the court case. The financial cost was almost \$10,000.

**Recommendation 7: Amend Nova Scotia’s access and privacy laws to make clear that a public body may first take a time extension of its own accord and can also ask the OIPC for additional time to respond similar to s. 10 of British Columbia’s *Freedom of Information and Protection of Privacy Act*.**

**(ii) The need for time extension requests**

It is critically important that public bodies respond to access requests in a timely manner. A common mantra is: “access delayed is access denied.” This is because outdated information can become irrelevant. It can compromise the public’s ability to meaningfully participate in the democratic process and hold public bodies to account.

Over the years, time extension requests from public bodies to the OIPC have increased dramatically. As demonstrated in the diagram below, time extension requests have increased from 13 per year in 2007 to 180 at the end of 2022-2023. While the time extension requests have gone down recently, the OIPC is seeing a corresponding increase in the number of deemed refusals.



Despite this vast increase in time extension requests, the Nova Scotia Government has declined to give the OIPC additional resources to complete this task.

Processing time extension requests is a big part of the work of the OIPC. In the first eight months of this fiscal year, the OIPC received 115 time extension requests. Of those requests, 85%<sup>9</sup> came through IAP Services from departments of the Nova Scotia Government (each government department is considered as a distinct public body). These departments are by far the biggest user of time extensions approved by the OIPC to respond to access requests.

<sup>9</sup> 98 out of 115.



The OIPC must respond quickly to time extension requests because there are strict timelines set out in the laws. Given these tight timelines, an OIPC investigator must stop working on a request for review file to respond to a time extension request.

The OIPC only has three access to information investigator positions. The resources that the OIPC dedicates to time extension requests is about the equivalent of one of those positions. What that means is one-third of the OIPC's access to information investigation staff cannot work on reviews relating to access to information requests because they must respond to so many time extension requests.

Time extension requests are time consuming. They are time consuming for the public body making the request because it must fill out a comprehensive form that provides its evidence to show that an extension is warranted. If the OIPC approves the time extension request, the public body must also take the time to write to the applicant to notify them of the time extension. They are also time consuming for OIPC staff who must review and assess the public body's information to decide whether to approve the time extension request. Finally, they take up time when applicants make requests for review.

Finally, time extensions are time consuming because of what the OIPC interprets as arising from cultural and/or financial reasons. The OIPC has issued [Time Extension Guidelines for Public Bodies](#) that clearly set out authorized circumstances for when the OIPC will permit a time extension. Despite this, and despite repeated reminders from the OIPC, public bodies continue to submit unauthorized circumstances as rationale for warranting a time extension. This eats up much of the OIPC's limited resources on long-decided practices.

Furthermore, when OIPC permission is not given, the OIPC often receives push-back and questions that attempt to challenge the OIPC's decision. OIPC staff are asked to provide additional reasons for their decisions, instead of the public body accepting the decision. There are also many requests to have the denial of time extension requests reconsidered.

Public bodies that ask for time extensions often do not do so because they meet the criteria in Nova Scotia's access and privacy laws such as, for example, because a large number of records was requested or needed to be searched and meeting the time limit would unreasonably interfere with their operations. By continuing to do this, it gives the impression that they do so because the public body can't keep up with the number of requests it is receiving or because there is disregard for the OIPC's statutory obligation to only grant time extensions that are permissible under the laws. Because of these actions, the OIPC's concern is that time extension requests are effectively being used as a case management tool.

Either more resources are needed to address this or public bodies, at the highest level, should be directing their staff to comply with most requests within the 30-day timeline required by the laws. A public body's use of a 30-day time extension on its own accord should be uncommon. Asking the OIPC for an additional time extension should be rare. This is not the case.

Frankly put, the overuse of time extension requests is not a good use of anyone's time. Public body time is better spent trying to get requested records out within the time frames set out in the laws. The OIPC's time is better spent on reviewing contested decisions of public bodies to deny applicants access to records.

Access requests are here to stay. Responding to them takes time, money, and clear direction from senior leadership that all information must be released, subject to the limited and specific exemptions written in the laws. As the amount and complexity of access requests increases, public bodies must increase their resources to respond to these increases, not make more time extension requests. The OIPC requires significantly more resources and the OIPC's perception is that public bodies do too.

The OIPC is also concerned that the Internal Working Group will consider extending time limits. The OIPC is strongly against any extension to time limits currently set out in Nova Scotia's access and privacy laws. Any extensions to time limits would make Nova Scotia an outlier in Canada. In terms of any need for legislative change, the issues with time extensions appear to be more related to resourcing than problems with the laws.

**Recommendation 8: Properly fund and resource public bodies, such as IAP Services and Nova Scotia Government departments, so that they have the capacity to process significantly more access requests without the need to take or request a time extension.**

**Recommendation 9: Address the culture of reliance on time extensions by setting clear direction to staff that they should only be used sparingly.**

**Recommendation 10: Properly fund the OIPC so that it has adequate resources to process time extension requests.**

**Recommendation 11: Do not amend Nova Scotia's access and privacy laws to extend time limits for responding to applicants' access requests.**

### **(iii) Additional time extension powers are needed**

The OIPC has noticed a trend where some applicants take up an above average amount of time communicating with public bodies and/or the OIPC. For example, they may send many emails or make many calls asking for things like immediate acknowledgements, clarifications on communications, and updates on their requests. They may also make many concurrent and/or close in time access request and/or requests for OIPC review. For example, recently the OIPC received 29 review requests from two applicants in a 14-month period. The OIPC has no way of knowing, but it is likely that these two applicants also made many more access requests to public bodies beyond only those that came to the OIPC for review.

While these actions would not likely amount to an abuse of process, public bodies and the OIPC are underfunded and so do not have the resources necessary to respond to these

types of applicants. As the OIPC states throughout this submission, more resources are needed to address this, and other problems. That being said, out of fairness to other applicants, it is also important to put some parameters around the amount of time that high volume users of the access regime take from public bodies and the OIPC. Other jurisdictions have also done so.<sup>10</sup>

Adding any permission to limit applicants' rights in these circumstances is an extraordinary remedy and so must only be done with oversight. To address the importance of not overusing the ability to limit access rights, Yukon has legislated that the Commissioner is allowed to permit a public body to take a time extension when an applicant has made multiple concurrent requests and responding to them "...would also unreasonably interfere with the responsive public body's operations." This approach is more modern and allows for flexibility if a public body did have the resources to respond to multiple concurrent requests.

**Recommendation 12: Amend Nova Scotia's access and privacy laws to, with the permission of the Commissioner, allow public bodies to take a time extension if an applicant initiates multiple concurrent requests to the same public body and responding to them would unreasonably interfere with the public body's operations.**<sup>11</sup>

In terms of the OIPC, the above-noted recommendation would be difficult to implement because who would oversee the Commissioner's choice? A different approach is needed. To reflect the large number of applicants who are waiting at least four years to have their review heard due to the OIPC's backlog, a fair approach would be to limit the number of reviews that the Commissioner must work on at one time for a particular applicant. This gives other applicants a chance to also access the services of the OIPC.

**Recommendation 13: Amend Nova Scotia's access and privacy laws to give the Commissioner the power to place review requests on hold where the applicant has five or more active reviews. Allow the Commissioner to hold additional review requests in abeyance and not commence an investigation until one of the five active complaints is resolved.**<sup>12</sup>

### ***Deemed refusal due to sign-off***

Over the last 14 years, the OIPC has witnessed a general trend of increasing deemed refusal reviews. A deemed refusal is when a public body fails to respond to an access request within the statutory timeline. The OIPC has reported on this worrying trend a number of times in its annual reports.<sup>13</sup>

---

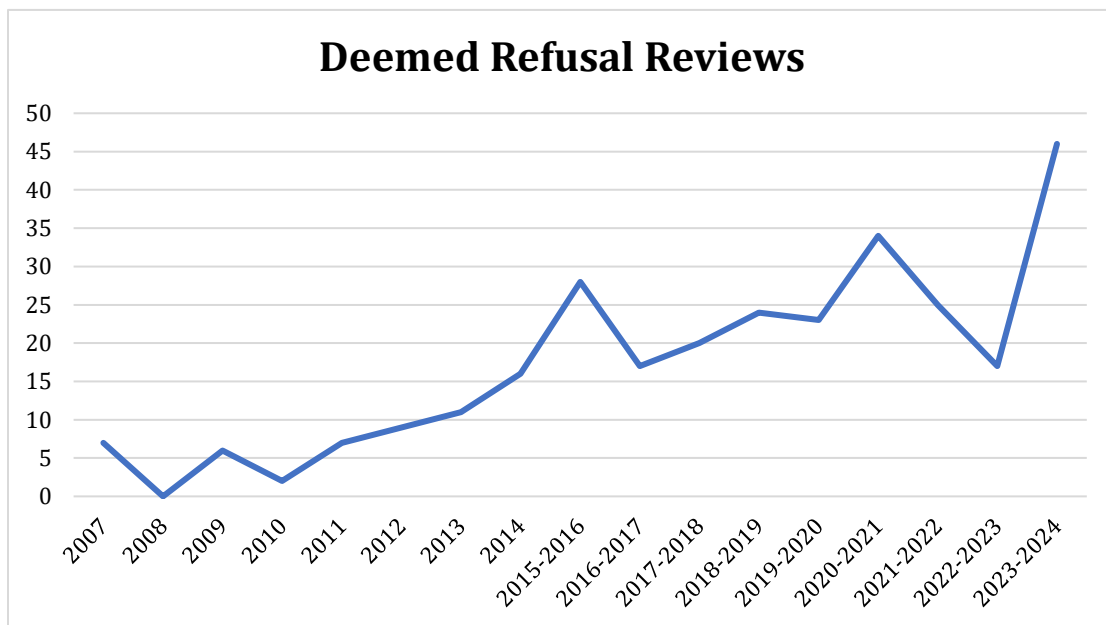
<sup>10</sup> See, for example, s. 14(2) of AB's *Freedom of Information and Protection of Privacy Act*, [RSA 2000, c F-25](#); s. 12(2) of PEI's *Freedom of Information and Protection of Privacy Act*, [RSPEI 1988, c F-15.01](#); and s. 62(2) of Yukon's *Access to Information and Protection of Privacy Act*, [SY 2018, c 9](#).

<sup>11</sup> Section 62(2) of Yukon's *Access to Information and Protection of Privacy Act*, [SY 2018, c 9](#).

<sup>12</sup> This is a power available to the Newfoundland and Labrador Office of the Information and Privacy Commissioner. See s. 44(7) of its [Access to Information and Protection of Privacy Act](#).

<sup>13</sup> The most detailed example is the OIPC's [2019-2020 Annual Report](#). See pp. 16 and 20.

When this happens, applicants can request a review from the OIPC, and the OIPC investigates the reasons for the delay. The chart below demonstrates the dramatic increase in demand for deemed refusal reviews by the OIPC. This chart does not demonstrate all the times that public bodies are in a deemed refusal position and applicants do not request a review from the OIPC. In other words, there are likely many more cases of public bodies being in a position of a deemed refusal than what is shown in the chart below.



Although many public bodies find themselves in a deemed refusal at some point or another, the Nova Scotia Government departments regularly explain the rationale for this delay as “waiting for sign-off”. This means that the decision still needs to be “signed-off” by someone in the department, typically a deputy minister. It is very rare to hear this reasoning from any other public body.

This isn’t a legitimate reason to not respond to an access request within the time required by the law.

**Recommendation 14: Implement a directive to all Nova Scotia Government department staff that responses to access requests cannot be delayed because they are waiting for sign-off.**

**Alternatively, amend Nova Scotia’s access and privacy laws to make clear that waiting for sign-off is not an authorized reason to delay responding to an access request.**

### ***Notices to third parties***

In some circumstances, Nova Scotia’s access and privacy laws require public bodies to give notice to third parties when the information being requested is third party personal

information or confidential business information. The wording of these sections is challenging to understand and could benefit from some clarity, however the law effectively says that notice to third parties is mandatory unless the public body (i) has sufficient evidence to support the application of a third party exemption and, after examining the views or interests of the third party, it has decided to refuse access to the record, or (ii) if giving notice is not practical.

The OIPC's view is that when the access and privacy laws say that the public body must examine the views or interests of the third party, this means it must collect this information from the third party. It cannot substitute its presumption of the third party's views or interests. The OIPC frequently sees public bodies, most notably Nova Scotia Government departments, deciding to not give a third party notice without any evidence that it has considered the views or interests of the third party.

The purpose of giving notice is to either get consent to disclose the information or to collect reasons for not disclosing it. Despite this, in the reviews that the OIPC conducts of public bodies' decisions to withhold information, public bodies (again, most notably Nova Scotia Government departments) frequently give discretionary notice to other public bodies or mandatory notice to organizations but rarely do when the requested records contain third party personal information of individuals. This is not right – why would another public body or organization be given this courtesy but not an individual? At times, this creates unfortunate and frankly heartbreaking outcomes for the applicant. For example, when applicants request records about their time in the care of the Government as a child, it is rare to see a public body give notice to the third parties mentioned in that person's records. Perhaps the third party might say, "No, I never want this person to know my involvement in their early life." Or they might say, "Yes, please give the information to the applicant. They should know more about their childhood." Despite the importance of this to the applicant, and the mandatory duty to give third party notices, public bodies don't, which can be baffling.

Another example is where an applicant's family member passes away in a workplace accident and there is a resulting investigation. It is entirely possible that a colleague of the deceased person might consent to the applicant knowing more about the circumstances of the death. And yet the OIPC has seen public bodies (again, most notably Nova Scotia Government departments) refusing to even ask these individuals for their consent despite it being mandatory to do so. When public bodies substitute their own views for those of the third parties, they deny applicants the possibility that a third party may consent to the applicant seeing that information. These decisions also do not follow the mandatory requirements set out in access and privacy laws. While the OIPC believes this is more of a cultural issue, given the seriousness of the impacts of not following this part of the law, explicit legislative changes are recommended.

**Recommendation 15: Amend Nova Scotia's access and privacy laws to make it clear that views or interests of third parties must be canvassed instead of assumed by public bodies when making disclosure decisions related to third party personal information or confidential business information.**

### *Anonymity of applicants*

Another issue that the OIPC wishes to address is the anonymity of applicants who request access to information. The identity of access to information applicants is personal information protected by access and privacy laws. The OIPC requested that the access and privacy laws be amended to protect the anonymity of access applicants in Recommendation 4 of the [2017 Special Report](#). But the OIPC is now of the view that even stronger protections in the laws are needed.

The Independent Review Committee that conducted the [Report of the 2014 Statutory Review on Access to Information and Protection of Privacy in Newfoundland and Labrador](#) had some interesting things to say about the issue of anonymity. At the time, before processing a request, access to information and protection of privacy (ATIPP) coordinators in Newfoundland and Labrador were required to complete a form that specified the applicant type in terms of belonging to the following categories:

- Academic/Researcher
- Business
- Individual
- Interest Group
- Legal Firm
- Media
- Other Public Body
- Political Party

The coordinators were also required to consult with communications staff with regard to any requests from the media. The Independent Review Committee said:

This type of involvement by staff impairs the fair operation of the access to information system. It suggests the motivation for this involvement has much to do with the image of the government of the day in news coverage. Nowhere in the *ATIPPA* is it stated that a valid reason for withholding information is how the government might be affected by media coverage of information disclosed through the Act.

....

The second observation is that the current system, where requests are scrutinized by staff, the deputy minister, and often the minister, facilitates the interpretation of *ATIPPA* in a partisan political way rather than in a fair, principled way.

The Independent Review Committee recommended that:

No officials other than the *ATIPP* coordinator be involved in the request unless they are consulted for advice in connection with the matter or giving assistance in obtaining and locating the information.

In response, Newfoundland and Labrador's [ATIPPA](#) was amended to include s. 12. This section clarifies that except in cases of personal information or in cases where the applicant has given consent, "The head of a public body shall ensure that the name and type of the applicant is disclosed only to the individual who receives the request on behalf of the public body, the coordinator, the coordinator's assistant and, where necessary, the commissioner."

The Nova Scotia Government [tracks](#) the type of applicants it receives access requests from in terms of the applicant being a business, a member of the media, a political party, a private individual, a public interest group, a third party representative, or "other". At a macro level, there is no problem with keeping track of the type of applicants. But at a micro level, unless an applicant is requesting their own information, the applicant's identity should be irrelevant in terms of deciding whether to release the requested information. The OIPC does not know if applicant types are translated to decision-makers at Nova Scotia Government departments or at any other public bodies. However, it is best to address this issue in case they are.

**Recommendation 16: Amend Nova Scotia's access and privacy laws to better anonymize the name and type of applicant within a public body similar to s. 12 of Newfoundland and Labrador's *Access to Information and Protection of Privacy Act*.**

### ***Limited and specific exemptions: non-responsive***

One of the purposes of Nova Scotia's access and privacy laws is to provide for the disclosure of all public body information with necessary exemptions that are limited and specific. These limited and specific exemptions are listed in the laws. Despite this requirement, there is a trend where public bodies do not rely on one of these exemptions to redact or withhold information, but instead rely on the basis that the records are "non-responsive".

Many applicants are wary of this approach. They think that public bodies are hiding information that is responsive to their access request and so they ask the OIPC to conduct a review of the public body's decision to withhold information on the basis that it is non-responsive.

The OIPC's view is that the existing laws effectively enable public bodies to withhold information that is truly non-responsive without the need to amend the laws. This is because if the applicant is not entitled to the information, it can be redacted or withheld using one of the existing exemptions. For example, if an applicant were to request their own personal information and the responsive document had other people's personal information on it, the public body may be required to redact or withhold that information under the personal information of a third party exemption. Or, if the requested record contained information that was non-responsive, but the public body would not have withheld it under another exemption, it could simply release that information to the applicant. The applicant could then determine for themselves that the information was non-responsive instead of worrying that it wasn't, but not knowing because the public body withheld it.

The Commissioner has issued several reports where she found that public bodies are not authorized to withhold information on the basis the information was non-responsive. For example, in [NS Review Report 21-09](#), she said:

[20] On multiple occasions, this office has examined the issue of whether or not public bodies are authorized under *FOIPOP* to determine that portions of responsive records are out of scope of the request and on that basis withhold those portions it deems to be non-responsive. In those cases, the former Commissioner carefully examined all of the current case law on this issue both for and against such a finding and concluded that Nova Scotia's *FOIPOP* does not permit public bodies to withhold information it deems to be "not responsive".

[21] The purpose of the legislation set out in s. 2 of *FOIPOP* is to provide the public with a right of access to "all government information" subject only to "necessary exemptions, that are limited and specific". Withholding information on the basis of "not responsive" or "out of scope" is not an exemption to the public's right of access set out in the legislation, like the exemptions set out in ss. 12-21 of *FOIPOP*.

[22] Using "not responsive" to sever snippets of information out of responsive records creates an unlimited, non-specific, entirely arbitrary exemption that frees the public body from any constraints created by the law. It fundamentally undermines the purpose and objectives of Nova Scotia's access to information legislation.

[23] The public body's representations cited old cases that have long been distinguished or rejected by this office. While using "not responsive" may arguably be permissible in other jurisdictions, without amendments to the legislation, it is not permitted here. No one disagrees that non-relevant documents need not be produced. However, once relevant documents have been identified, information within them can only be redacted subject to the exemptions set out in *FOIPOP*. I suggest that this practice end once and for all.

[24] For the reasons set out above, I find that "not responsive" cannot be used to remove information from the record.

In 2022, the Supreme Court of Nova Scotia rejected the OIPC's interpretation. In [Raymond v. Halifax Regional Municipality](#), the Judge disagreed with the Commissioner's approach. The Judge said:

I disagree with the OIPC finding. It is illogical to say that non-responsive information could be withheld if it was in a completely separate document but can be disclosed if contained in a document that also contains responsive information. In support of my position I rely on the decision of Justice Scanlan (as he then was) in *Stevens v. Nova Scotia (Department of Labour and Workforce Development)*, 2012 NSSC 367. [see para. 76]



Unless it is distinguishable, the OIPC is required to, and does, follow the decisions of Nova Scotia courts and the Supreme Court of Canada (and often also courts from other jurisdictions, although it is not required to).

**Recommendation 17: Amend Nova Scotia’s access and privacy laws to make it clear whether public bodies can or cannot withhold information based on the information being “non-responsive” by creating that authority as a limited and specific exemption. If an amendment is made to include “non-responsive” as an exemption, include a definition of this term.**

### *Indigenous issues*

Nova Scotia’s access and privacy laws set out two sections specific to Indigenous information:

- Under s. 12(1)(a)(iii) of [FOIPOP](#) and 472(1)(a)(v) of the [MGA](#), a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to harm the conduct by the Government of Nova Scotia of relations between the Government and an Aboriginal government.
- Under s. 20(2)(d) of [FOIPOP](#) and s. 480(2)(d) of the [MGA](#), if disclosure of personal information constitutes an unreasonable invasion of a third party’s personal privacy, a public body must consider whether the disclosure would assist in researching the claims, disputes, or grievances of Aboriginal people.

Though these sections of Nova Scotia’s access and privacy laws are valuable for Indigenous communities, significant time has passed since these laws have been enacted or amended. As a result, Nova Scotia’s access and privacy laws may not reflect the current needs of Indigenous communities that have been brought to light over the past 30 years.

In 2021, the Government of Canada had an [Indigenous-specific engagement process](#) to seek input on modernization of the federal [Access to Information Act](#) and the [Privacy Act](#). This process was critical for the Government of Canada to understand and address the unique issues and concerns with access to information from Indigenous peoples.

Due to this engagement process, three key themes emerged as relevant issues for Indigenous communities: the need for Indigenous data sovereignty, improvements to Indigenous peoples’ right of access, and the need to expand the definition of “Indigenous government”.

In addition, the Newfoundland and Labrador Commissioner’s [submission](#) for the 2020 review of its [ATIPPA](#) examined whether there were any special access to information and protection of privacy issues in Indigenous communities that deserve attention, and if so, should those concerns be addressed within [ATIPPA](#), or should they be addressed within the legal frameworks of those communities. The Commissioner recommended consultations

with Indigenous communities and other relevant stakeholders to determine how [ATIPPA](#) could better address their needs and expectations.

Reconciliation is still an ongoing process of establishing and maintaining respectful relationships. This Legislative Review opens an opportunity for the Nova Scotia Government to better address and support the interests of the Indigenous community. Though this issue might fall outside the mandate of this Legislative Review, the OIPC believes it is important for the Internal Working Group to consult with relevant stakeholders and consider their views on whether any amendments should be made to Nova Scotia's access and privacy laws to reflect the needs of Indigenous peoples and communities.

**Recommendation 18: Initiate consultation with Indigenous organizations, Indigenous governments, and other relevant stakeholders to consider whether Nova Scotia's access and privacy laws can better reflect the needs and expectations of Indigenous people.**

**Recommendation 19: Create a definition of "Indigenous government" that would better encompass Indigenous governments and organizations in Nova Scotia.**

### ***Compassionate disclosure***

The OIPC often gets review requests from applicants who are seeking to access information about the death of their loved one. Grieving people often turn to access and privacy laws to get information about a loved one's death when they cannot get the information in another less formal way from a public body.

An applicant's deceased loved one is considered a third party. Third parties have privacy rights under access and privacy laws. They retain privacy rights after their death, although those privacy rights diminish over time. Third parties' privacy rights need to be balanced against the grieving applicants' access rights. It is not black and white.

When deciding if it would be an unreasonable invasion of a deceased individual's privacy if their personal information was released to a loved one, the access and privacy laws require that the public body consider all relevant circumstances, including a non-exhaustive list of specific circumstances. Although this list is non-exhaustive and there are review reports that explain this, public bodies can still at times be resistant to considering factors that are not on the list.

Unlike some other jurisdictions, Nova Scotia's access and privacy laws do not specify that public bodies must consider compassion as a relevant circumstance when contemplating disclosure. Nevertheless, because the list is non-exhaustive, the Commissioner has found many times that it is relevant and should be considered. For example, in [NS Review Report 16-08](#), the Commissioner carefully considered the concept. She noted research has shown that understanding all the details about the death of a loved one is a fundamental part of

grieving. She noted adjudicators in Ontario have concluded that greater knowledge of the circumstances of a loved one's death is, by its very nature, compassionate.<sup>14</sup> Being denied personal information about a loved one's death can be very difficult and frustrating for applicants.

Other provinces such as Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Prince Edward Island, and Newfoundland and Labrador have included provisions relevant to compassionate disclosure. Section 14(4) of Ontario's [Municipal Freedom of Information and Protection of Privacy Act \(MFIPPA\)](#) is particularly well written. It provides that a disclosure does not amount to an unjustified invasion of personal privacy if it discloses information about a deceased individual to a spouse or a close relative of the applicant, and the public body is satisfied the disclosure is desirable for compassionate reasons. There is no weighing of factors; it is considered as not being an unjustified invasion of the third party's privacy.

**Recommendation 20: Amend Nova Scotia's access and privacy laws to state that disclosure does not amount to an unjustified invasion of personal privacy if it discloses information about a deceased individual to a spouse or a close relative of the deceased individual, and the public body is satisfied disclosure is desirable for compassionate reasons.**

**Alternatively, amend Nova Scotia's access and privacy laws to include compassion as a relevant circumstance to consider when weighing whether disclosure of third party personal information would be an unreasonable invasion of their personal privacy.**

## C. Modernizing privacy rights

The growth in data-driven technologies has exploded in recent years. These technologies undoubtedly bring great benefits to citizens, but they also come with great risks. Nova Scotia's access and privacy laws are particularly lacking and fall short of the rigorous and substantive privacy protections seen in other jurisdictions across the country in this regard. The OIPC encourages the Internal Working Group to fully address updates in technology in relation to privacy.

### ***Definition of "use of personal information"***

Although the word "use" is found throughout access and privacy laws, it is not a defined term in them. In more modern pieces of legislation, the term "use" is defined. For example, Nova Scotia's [PHIA](#) defines "use" as, "...to handle or deal with the information, but does not include to disclose the information."

Newfoundland and Labrador's [Personal Health Information Act](#) is even more clear. It defines "use" as, "...to handle or deal with the information or to apply the information for a purpose

---

<sup>14</sup> See, for example, *ON Order MO-2245, Halton Regional Police Services Board (Re)*, [2007 CanLII 82541 \(ON IPC\)](#).

and includes reproducing the information, but does not include disclosing the information.” Having defined terms makes Acts easier to understand and follow and so a definition of “use” would be helpful.

**Recommendation 21: Amend Nova Scotia’s access and privacy laws to include a definition of “use” of personal information consistent with that found in Newfoundland and Labrador’s *Personal Health Information Act*.**

**Alternatively, set out a definition that is consistent with Nova Scotia’s *PHIA*.**

### ***Young people’s privacy***

The online world presents many good things for young people, but it is accompanied by many risks to them. Young people are more prone to these risks than adults. They can also be hurt in different ways than adults. Most critically, young people can also be exploited or threatened by bad actors who use their digital personal information to cause them harm. There are too many tragic stories of children harming themselves for fear of bad actors posting extremely private personal information about them online.

In October 2023, Canadian Information and Privacy Commissioners issued a joint resolution titled [\*Putting best interests of young people at the forefront of privacy and access to personal information\*](#). This resolution lists numerous policy and legal instruments that have been implemented across the world to address young people’s privacy rights and ways to protect them in the online world. However, it notes that there is still much to be done in Canada to protect young people through legislative means.

**Recommendation 22: Amend Nova Scotia’s access and privacy laws to be consistent with international legal instruments that attempt to ensure adequate protection of young people’s privacy rights that protect them from the risks of the online world.**

### ***Who can act for a child and young people***

Young people have access and privacy rights. They can make choices about them. However, the access and privacy laws are vague in terms of what age a young person has the capacity to exercise their access rights and make decisions in relation to their privacy rights. When does application of these rights shift from a parent or guardian to their child?

The [\*Convention on the Rights of the Child\*](#) defines a child as a human being under the age of 18, unless national laws recognize an earlier age of majority.

According to s. 54(c) of Ontario’s [\*MFIPPA\*](#), an individual having lawful custody of a child under 16 years of age may provide consent on the child’s behalf to file a privacy complaint and exercise all rights and powers of individuals set out in the legislation. However, once a child turns 16, their parent or guardian may no longer consent on their behalf.

Section 104(1)(c) of Alberta's [Health Information Act](#) states that if an individual wishes to act on behalf of their child, they are required to demonstrate that their child is under 18 years of age and does not understand the nature of the right or power and the consequences of exercising that right or power.

In its [Guidelines for obtaining meaningful consent](#), the federal Office of the Privacy Commissioner of Canada takes the position that anyone under the age of 13 would require their parents or guardian to help them make privacy-related decisions.

According to the [Age of Majority Act](#), in Nova Scotia, you are a minor if you are under 19 years of age and a child if you are under 16 years of age. Nova Scotia's access and privacy laws state that any right or power conferred on an individual by the legislation may be exercised where the individual is less than the age of majority, by the individual's legal custodian in situations where, in the opinion of the head of a public body, the exercise of the right or power would not constitute an invasion of privacy of the individual.

This is a good start, but individuals under the age of 19 have different levels of maturity and different intellectual and developmental abilities. As maturity increases, a child can make more independent decisions and express what is in their best interests. Furthermore, a child's capacity to consent and make decisions can vary from individual to individual. There should be flexibility in the laws to acknowledge these variances.

**Recommendation 23: Amend Nova Scotia's access and privacy laws to include provisions that address when an individual under the age of 19 can exercise their access and privacy rights.**

### ***PIIDPA***

The purpose of Nova Scotia's [Personal Information International Disclosure Protection Act](#) is to require that personal information be stored in Canada. It prohibits disclosure (with certain exceptions) of personal information outside of Canada. Effectively, this prevents public bodies from using cloud storage because that would mean that personal information is disclosed outside of Canada. The problem is that *PIIDPA* has no oversight requirements. What that means is if a public body contravened *PIIDPA*, the affected person has no right to complain to the OIPC.

At one time, only Nova Scotia and British Columbia had these sorts of restrictions. In 2021, British Columbia amended its [FIPPA](#) by removing the prohibition (with some exceptions) on disclosure of personal information outside of Canada. It's important to note that the amended legislation still requires public bodies to protect information stored or disclosed outside of Canada by having reasonable security arrangements in place. This is critically important because once personal information leaves Canada, Canadian laws no longer apply. This makes the requirement to protect personal information when it is stored or disclosed outside of Canada even more important.

**Recommendation 24: Review whether the provisions of the *Personal Information International Disclosure Protection Act* would benefit from any amendments. Put all storage and disclosure of personal information outside of Canada provisions within one combined access and privacy law so that there will be a means for independent oversight and all storage and disclosure of personal information outside of Canada will be required to follow the same safety requirements set out in Nova Scotia’s existing access and privacy laws.**

### ***Emerging issues and technologies***

Data-driven technologies that rely on the collection, use, and disclosure of personal information are rapidly changing. These changes can bring great benefits to individuals. They can improve things like health care, economic growth, and government efficiencies. But without proper regulation, these technologies could cause harm. These innovations should be enabled but in a way that protects access and privacy rights. Making amendments in this regard will be challenging for governments as changes need to be made that provide for effective protections without being too prescriptive so that continued evolution and development can take place.

This submission addresses some of the main emerging technologies that should be addressed.

#### **(i) Automated decision-making, artificial intelligence, and generative artificial intelligence**

Businesses and governments around the world have begun or are beginning to use automated decision-making and artificial intelligence (AI) in their work.

Automated decision-making systems use rule-based or predetermined instructions to analyze and make inferences or decisions from large amounts of data. They either assist or replace the judgment of human decision-makers.

AI can learn from data, make decisions based on it, and make predictions from it. It can perform tasks that would normally require human brain power to complete. Generative AI is “...a subset of machine learning in which systems are trained on massive information sets – often including personal information – to generate content such as text, computer code, images, video, or audio in response to a user prompt.”<sup>15</sup>

In simpler terms, these technologies essentially assist or replace the judgement of human decision-makers with automated decision-making tools. These technologies do not simply make application systems faster. Instead, they can analyze and process applications differently, sometimes in ways that are not always clear to the implementor or the user.

---

<sup>15</sup> Joint Statement of the Federal, Provincial and Territorial Information and Privacy Commissioners *Principles for responsible, trustworthy and privacy-protective generative AI technologies* (December 7, 2023), online: <[https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd\\_principles\\_ai/#fn2](https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/#fn2)>.

Authorities around the world are recognizing that while these automated tools provide many positive benefits, they also pose serious privacy risks. In 2019, the Government of Canada implemented a [Directive on Automated Decision-Making](#) which provides minimum requirements for federal government departments that wish to use an automated decision system. These requirements focus on the need for algorithmic impact assessments, transparency, quality assurance, recourse, and reporting.

In June 2023, the G7 data protection and privacy authorities issued a joint [Statement on Generative AI](#).

In October 2023, the Global Privacy Assembly issued a [Resolution on Generative AI Systems](#).

In November 2023, a [G7 Leaders' Statement](#) included guiding principles and a code of conduct for organizations developing AI systems.

In December 2023, all Canadian Privacy Commissioners released [Principles for responsible, trustworthy and privacy-protective generative AI \(artificial intelligence\) technologies](#). In this document, Canadian Commissioners noted that while generative AI tools may pose new risks to privacy and concerns about the collection, use, and disclosure of personal information, such tools do not occupy a space outside of current legislative frameworks – they must still comply with applicable privacy laws and regulations in Canada. That being said, particularly with Nova Scotia's dated laws, there may be room for some legislative improvements in terms of automated decision-making, AI, and generative AI.

The OIPC does not know if public bodies in Nova Scotia have or intend to implement such tools or if any directives have been issued to Nova Scotia Government departments regarding their use. Any legislative amendments in this regard will be challenging in light of the fast rate of expansion of these technologies around the world, however the OIPC would be remiss if it did not encourage the Internal Working Group to research and address whether legislative changes are warranted.

**Recommendation 25: Canvass the privacy concerns associated with automated decision-making, AI, and generative AI, and consider whether legislative amendments are required to address this emerging technology. Consideration should be given to whether Nova Scotia's access and privacy laws should be amended to:**

- a) Incorporate definitions of automated decision-making, AI, and generative AI.
- b) Require that algorithmic assessments and privacy impact assessments be conducted prior to the implementation of any projects or programs involving the use of automated decision-making, AI, or generative AI.
  - i) Require these assessments be provided to the OIPC for comment prior to implementation.
- c) Set out “no-go zones” for the use of automated decision-making, AI, or generative AI, such as the creation of projects or programs for malicious purposes.

- d) Give individuals the right to be notified when automated decision-making technologies are being used to make decisions about them.
- e) Give individuals the right to object to the use of automated processing of their information.
- f) Require public bodies to have technology that allows them to create a traceable record of how a decision was made.
- g) Disclose the reasons and criteria used for any automated decision.

## **(ii) Biometrics**

One of the most sensitive forms of personal information is biometric information. Article 4(14) of the European Union's [General Data Protection Regulation](#) defines biometric data as:

'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Biometric information (sometimes referred to as biometric data or biometric characteristics) is mostly unique to each person. For example, each person has unique irises. On the other hand, some biometric characteristics, like facial features, may be more similar among some people. Some biometrics tend to be stable over time and are difficult to alter (like irises). Others, like faces, tend to change over time and can also be altered by things like surgery or disguises.

There is a growing interest in using biometric information to identify people or verify their identity. The use of biometric information has much positive potential in terms of improving citizen-centric service delivery. However, it also creates some of the most significant privacy risks given the uniqueness of the information.

The risks of technology associated with biometric information have been comprehensively set out by Newfoundland and Labrador in a document titled [Submission of the Information and Privacy Commissioner to David B. Orsborn, Committee Chair of the ATIPPA Statutory Review Committee 2020 on the Review of the Access to Information and Protection of Privacy Act \(ATIPPA, 2015\)](#). This submission need not be repeated here, however the OIPC recommends that the Internal Working Group review it as well as the legislative amendments that have been implemented in other jurisdictions, such as Prince Edward Island, Alberta, and Quebec. This sensitive information should be better protected in Nova Scotia's access and privacy laws.

**Recommendation 26:** Amend Nova Scotia's access and privacy laws to include a definition of "biometric information" and to set out the significant independent oversight mechanisms that this very sensitive information warrants.



### **(iii) Data linking**

In Recommendation 13 of the [2017 Special Report](#), the OIPC addressed the issue of combining or matching personal information data from different data sets. This concept has varied names such as data linking, data matching, and data sharing for common or integrated programs and activities. This submission refers to it as data linking.

Data linking has many benefits. It can improve the delivery of citizen-centered services. However, it can also come with many risks. In 2017, the Office of the Saskatchewan Information and Privacy Commissioner issued a [detailed paper](#) on its recommendations for legislative change. It is a comprehensive document that the OIPC encourages the Internal Working Group to consider. Although not yet proclaimed in force, in 2018, Saskatchewan passed [The Data Matching Agreements Act](#) to govern this kind of activity. In 2019, Ontario amended its [legislation](#) to authorize and put parameters on integrating data across ministries and other publicly-funded organizations. As required by those amendments, in 2021, the Ontario Ministry of Government and Consumer Services issued [Ontario Public Service Data Integration Data Standards](#).

There have been several developments in this area since the OIPC issued its recommendations in the *2017 Special Report*. These developments predominantly address concerns related to transparency and privacy protections for data linking (as well as oversight as addressed in the *2017 Special Report*). In [its submission on proposed legislative change](#), the Office of the Information and Privacy Commissioner for British Columbia recently set out additional ways that legislation can protect privacy and transparency related to data linking by:

- “bringing transparency to these initiatives through public notice or reporting;
- creating protections through technical safeguards, such as rules on encryption, de-identification, limiting the retention of personal information in order to not to store duplicate copies of databases or to create new large repositories of personal information from linked data;
- administrative requirements, such as the need for formal agreements between public bodies when engaging in joint data-linking initiatives;
- requirements to ensure that the personal information used and created about citizens is accurate; and
- the provision of oversight by requiring certain documentation to be sent to or made available to the regulator.”

**Recommendation 27: Review data linking legislative developments in other jurisdictions and include provisions in Nova Scotia’s access and privacy laws that address the concept of data linking in terms of transparency, privacy protections, and oversight.**

## D. Improving oversight

### *Independence of the OIPC: funding*

In Recommendation 22 of the [2017 Special Report](#), the OIPC commented on the problems associated with Nova Scotia being the only jurisdiction in Canada that has not made its Information and Privacy Commissioner an independent officer of the House of Assembly. The problems associated with this permeate almost every aspect of the OIPC's work. The most significant and tangible of these is the Commissioner's lack of independence in terms of funding.

The Commissioner must seek budget approvals through a Nova Scotia Government department she oversees – the Department of Justice. This is unlike independent officers of the House of Assembly, such as the Auditor General. Independent officers make their requests to an all-party committee, who then makes recommendations to the Nova Scotia Government. These recommendations can be rejected but the opposition party is made aware of this.

In Nova Scotia, the budget (also called the estimates) is introduced in the House of Assembly by the Nova Scotia Government for a vote in the Legislature.<sup>16</sup> The OIPC's budget is not before the House as a standalone document for debate. It is put forward through the Department of Justice.

The current Commissioner has made budgetary requests for sufficient staffing each year since her term began in 2020. All requests have been denied. This is problematic. Since 2013, the Nova Scotia Government has been well aware that the OIPC has had a backlog. This Commissioner inherited a four-year backlog in 2020 and has not been able to reduce it. And yet, the Government refuses to provide the OIPC with sufficient funding to address this unacceptable backlog. A better model would be for the OIPC to have more independence in terms of its funding to ensure that it has adequate staffing to fulfill its duties. An example of this is in British Columbia's [FIPPA](#), which provides:

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

---

<sup>16</sup> <https://novascotia.ca/budget/budget-primer/>

The OIPC long ago reached the limit of what it can do with its current funding. While this may sound dramatic, the extraordinary impacts of the OIPC's lack of funding are dramatic. OIPC staff strongly believe in the importance of the public's access and privacy rights. They know that the four-year backlog flies in the face of those rights. Seeing the system deteriorate in Nova Scotia is frustrating and demoralizing for OIPC staff. But it is even more so for the public. Some applicants drop their request for review when the OIPC gets to their file because so much time has passed. The OIPC has been told that some applicants don't even bother to request a review because they know that by the time the OIPC can work on their file, the information will no longer be useful. This is appalling. Something needs to be done to amend the OIPC's budgetary process so that it can obtain sufficient resources to effectively conduct its work.

**Recommendation 28: Amend Nova Scotia's access and privacy laws to give the OIPC financial independence.**

***Reasons for rejecting the Commissioner's recommendation(s)***

At the conclusion of an access review or privacy investigation, the Commissioner issues recommendations for the public body to resolve the applicant's request for review.

In 2022-2023, the OIPC issued 11 review reports with 21 recommendations. Seventeen of those recommendations found in favour of disclosure. Public bodies accepted 11 or 65% of those recommendations. The acceptance rate has fluctuated significantly over the years.

Nova Scotia's access and privacy laws do not require public bodies to provide their rationale for rejecting the Commissioner's recommendations. Despite this, public bodies do at times explain their rationale when rejecting recommendations, which is appreciated by the OIPC and presumably by applicants. However, with some exceptions, these rationales are typically limited to statements along the lines of, "The public body takes its responsibilities seriously but stands by its original decision." In other words, there is no explanation for *why* the public body rejected the detailed analysis and recommendation(s) set out in the review report.<sup>17</sup>

Unlike in Nova Scotia, s. 104 of Yukon's recently updated [Access to Information and Protection of Privacy Act](#) includes a requirement that the public body must provide reasons when rejecting Commissioner<sup>18</sup> recommendations.

---

<sup>17</sup> If the Internal Working Group would like to see some examples where the rejection is insufficient to understand the legal basis for it, the OIPC would be happy to provide anonymized letters.

<sup>18</sup> Note that in the Yukon, adjudicators (and not the Commissioner) write review reports.

In [\*VinAudit Canada Inc v Yukon \(Government of\)\*](#), the Supreme Court of Yukon Judge had some strong words about the public body's response to the recommendations issued by the Yukon Office of the Information and Privacy Commissioner. The Judge said:

[69] More generally, the Decision provides no reasoning or analysis beyond a reciting of its earlier position. It fails to consider or rebut the Report's 58 paragraphs (15 pages) of factual and jurisprudential analysis, or its specific analysis of the data fields explaining why the information neither constitutes "personal information" nor would reveal personal information, thereby requiring its non-disclosure under s. 70 of the Act.

...

[87] To conclude, apart from "respectfully disagree[ing]" with the adjudicator's recommendations and analysis, and its inapposite citation of *Philip Morris*, the Decision does not consider or rebut the comprehensive analysis of the adjudicator's Report. The Decision fails to provide a transparent, intelligible, justifiable, and reasonable basis for rejecting the contents of that Report: it largely ignores them. **The respondent's perfunctory and conclusory four-paragraph response to the thorough 47-page Report borders on contempt towards the presumptive right of the Yukon public to government information, towards the statutory regime designed to facilitate that access, and towards the Office of the Commissioner statutorily entrusted to uphold that legislation and realise its goals.** [emphasis added].

This is not a problem unique to this Yukon department. From the OIPC's experience, a similar culture exists in Nova Scotia. There is a culture of disregard for access and privacy laws, and for the expertise and work of the OIPC in its mandate to ensure those laws are upheld.

In contrast, the OIPC puts significant time, research, and analysis into informal resolution efforts and in review reports if informal resolution is not successful. OIPC documents provide a detailed analysis of why the access and privacy laws do or don't authorize disclosure of the requested information. They also fulsomely explain how the common law has interpreted access and privacy laws. In response, most public bodies do not explain how or why the access and privacy laws allow them to withhold the requested information. The law doesn't require them to. Response letters from public bodies typically just say that they disagree, with no explanation why. The result is that applicants never get an explanation for how public bodies are allowed to make these decisions that frequently reject years of decisions from the OIPC, other Information and Privacy Commissioners' offices from across the country, and the Supreme Court of Nova Scotia. The OIPC can only imagine how disappointing this is for applicants. They wait at least four years for the OIPC's review. The OIPC provides considerable detail for its recommendations, and then public bodies disagree and don't give a justifiable explanation.

The OIPC's view is that not having a legislative requirement for public bodies to provide reasons for rejecting the Commissioner's recommendation(s) is contrary to the presumptive right of individuals to access government information, frustrates the statutory

regime designed to facilitate that access, and shows disregard towards the OIPC who is statutorily entrusted to uphold the legislation.

Furthermore, a significant number of OIPC review reports say the same thing – that the OIPC has told the public body many times that it cannot withhold information in that fashion. In the context of the OIPC's significant backlog, repeatedly pushing matters forward to OIPC review when the matter has been previously settled is particularly problematic. The OIPC's work is bogged down by repetitive review reports. This frustrates the ability of the OIPC to focus on complex issues and unsettled areas of law. The OIPC's resources would be much better used if it was not forced to repeatedly issue reports that say the same thing.

The OIPC's view is that requiring public bodies to fulsomely explain their rationale for refusing the Commissioner's recommendation(s) will not only serve the public interest but may also reduce the need for repetitive review reports. This is because if a public body cannot rationally explain why it disagrees with the Commissioner's recommendation(s), then perhaps it may not continue to withhold information in future similar circumstances.

**Recommendation 29: Amend Nova Scotia's access and privacy laws to require that public bodies must provide transparent, intelligible, justifiable, and reasonable reasons for rejecting any of the Commissioner recommendations.**

### ***Role of access and privacy administrators***

Nova Scotia's access and privacy laws designate the head of the public body as being responsible for all the requirements set out in them. However, the norm is that these obligations are carried out in some ways by access and privacy administrators.

Public bodies in other jurisdictions have taken different approaches to the organization of access and privacy administrators. In some jurisdictions, there is a separate administrator for each public body. In other jurisdictions, the administrators are centralized into one unit where they help all or some of the public bodies within that jurisdiction with the access requests and privacy complaints they received.

Typically, a centralization approach only happens with large public bodies, such as provincial or municipal governments.

The Nova Scotia Government has taken the centralization approach. In 2015, Information Access and Privacy (IAP) Services was formed to centralize information access and privacy administrators into one unit. These administrators are then assigned to assist Nova Scotia Government departments. One of the main mandates of IAP Services is to provide support to Nova Scotia Government departments on how to respond to both access requests and privacy complaints, as well as how to respond when applicants request a review from the OIPC.

Because the OIPC conducts the majority of its reviews on decisions made by Nova Scotia Government departments, this part of the submission will use specific examples from the OIPC's experiences with Nova Scotia Government departments serviced through IAP Services during the review process. However, this commentary is applicable to any public body using a centralized approach.

During a review, IAP Services' administrators act as a liaison between their client departments and the OIPC. When the OIPC is reviewing the matter, the OIPC investigator (who is delegated by the Commissioner to investigate and attempt informal resolution) communicates with IAP Services' administrators, not someone within the department.

Delegations to IAP Services' administrators are permitted under the laws. The OIPC's understanding is that most departments have delegated at least some of their powers and duties to IAP Services, but the OIPC is entirely in the dark as to which departments have delegated their powers to IAP Services, which have not, and whether the delegations place any restrictions on the exercise of those powers by IAP Services' administrators. The laws require these delegations to be in writing, however they are not made public, and they are not provided to the OIPC.

In 2014, Newfoundland and Labrador commissioned an [independent review](#) of its *ATIPPA*. This review contained some valuable observations about the status, or lack of status, of its ATIPP coordinators. In a nutshell, the independent review noted that having a centralized service is not a magic bullet. Centralization can bring both good and bad. It said that when ATIPP coordinators are fully delegated departmental powers and duties, or fully engaged with senior decision-makers in the department, the outcomes are typically better than when they appear to essentially be carrying messages back and forth. On the other hand, when ATIPP coordinators are given little delegation, decisions are often made based on partisan, political rationales rather than on the requirements of the laws.

To address these issues, the Newfoundland and Labrador Independent Review Committee recommended:<sup>19</sup>

2. The *Act* be amended to give delegated authority for handling a request solely to the ATIPP coordinator.
3. No officials other than the ATIPP coordinator be involved in the request unless they are consulted for advice in connection with the matter or giving assistance in obtaining and locating the information.
4. The *Act* be amended to anonymize the identity and type of requester upon receipt of the request and until the final response is sent to the requester by the ATIPP coordinator, except where the request is for personal information or the identity of the requester is necessary to respond to the request.

---

<sup>19</sup> These recommendations on p. 47 of the Newfoundland and Labrador [Report of the 2014 Statutory Review of the Access to Information and Protection of Privacy Act](#) begin with Recommendation #2.

Subsequently, in a [2020 review](#) of Newfoundland and Labrador's current [ATIPPA](#), the Newfoundland and Labrador Commissioner noted that these recommendations were not implemented, but that "...it would be a good idea to explore options to enhance the authority and compensation level of [ATIPP] Coordinators."

The OIPC echoes these recommendations and suggestions. It is very challenging to work with administrators such as those at IAP Services when it is not known if they have decision-making authority. Are IAP Services' administrators given decision-making authority or are they not? If they are not, is anything being lost in translation?

Access and privacy administrators should have significant expertise in the laws. They are tasked with conducting valuable work in a fast-paced, stressful environment. But if they are not given delegated authority, then what are they to do if the decision-maker tells them to contravene the law? The OIPC doesn't know if this is happening with IAP Services' administrators and Nova Scotia Government departments, or any other public bodies. What is known is that positions and arguments that anyone with expertise in this area should well know do not comply with the law are regularly advanced anyway. This is unfortunate and it also eats significantly into the use of the OIPC's limited resources. It needs a remedy.

Whoever is responsible for decision-making should be the liaison with the OIPC. Otherwise, the process becomes like a game of telephone and the OIPC worries that its expertise may inadvertently be missed in it.

In the OIPC's view, the best solution to this is to give IAP Services' administrators (and all public body access and privacy administrators) the power and autonomy to implement decisions that comply with access and privacy laws. They have the expertise to do so, and decisions would be unlikely to be viewed as partisan if they were the decision-makers as opposed to departments. This is a serious job. If this recommendation is implemented, their compensation should be increased to reflect that role. This would likely also help with attracting and retaining administrators.

Finally, the OIPC would be remiss to not suggest that its staff also be given increased compensation to reflect their delegated roles. Doing so would help the OIPC attract and retain access and privacy staff.

**Recommendation 30: Explore options to enhance the decision-making powers of IAP Services' administrators. If they are expanded, increase their compensation to reflect their expertise and job requirements.**

**Recommendation 31: Explore options to increase the compensation of OIPC staff to reflect their expertise and job requirements.**

### ***Powers of the Commissioner***

Recommendation 32 of the [2017 Special Report](#) suggested several improvements to the powers of the Commissioner. Other, more modern pieces of legislation contain even more powers than those recommended in the *2017 Special Report*. An example of this is s. 42 of British Columbia's [FIPPA](#) which grants the Commissioner the ability to do things like:

- receive comments from the public about the administration of the legislation;
- engage in or commission research into anything affecting the achievement of the purposes of the legislation;
- bring to the attention of the head of a public body any failure to meet the prescribed standards for fulfilling their duty to assist applicants.

These are just some of the many additional powers granted to Commissioners in other Canadian jurisdictions. A jurisdictional scan should be undertaken and general powers from other more modern pieces of legislation should be added to Nova Scotia's access and privacy laws.

**Recommendation 32: Amend Nova Scotia's access and privacy laws to give the Commissioner the same general powers that are commonplace in more modern Canadian legislative schemes.**

### ***Other minor improvements***

There are a few areas of Nova Scotia's access and privacy laws where minor changes could be made to improve clarity. The OIPC's recommendations in this regard are not policy-based or contentious. Rather, they are more of an administrative matter. Rather than lengthen this submission, the OIPC will provide these minor suggestions to the Internal Working Group.



## Appendix A - List of recommendations

**Recommendation 1:** Ensure that the privacy provisions in *PRO* are combined with all other Nova Scotia access and privacy laws into one complete Act.

**Recommendation 2:** Amend Nova Scotia's access and privacy laws to make political parties subject to the personal information and oversight rules set out in them.

**Recommendation 3:** Amend Nova Scotia's access and privacy laws to include a definition of the term "prosecution" and clarify when it starts.

**Recommendation 4:** Amend Nova Scotia's access and privacy laws to include a definition of the phrase "exercise of prosecutorial discretion".

**Recommendation 5:** Amend Nova Scotia's access and privacy laws to ensure there is clear, explicit, and unequivocal language that the Commissioner can require production and examination of all records to which the solicitor-client privilege exemption has been applied by a public body.

**Recommendation 6:** Amend Nova Scotia's access and privacy laws to make clear that settlement privilege is not an exemption under which public bodies can withhold information.

**Recommendation 7:** Amend Nova Scotia's access and privacy laws to make clear that a public body may first take a time extension of its own accord and can also ask the OIPC for additional time to respond similar to s. 10 of British Columbia's *Freedom of Information and Protection of Privacy Act*.

**Recommendation 8:** Properly fund and resource public bodies, such as IAP Services and Nova Scotia Government departments, so that they have the capacity to process significantly more access requests without the need to take or request a time extension.

**Recommendation 9:** Address the culture of reliance on time extensions by setting clear direction to staff that they should only be used sparingly.

**Recommendation 10:** Properly fund the OIPC so that it has adequate resources to process time extension requests.

**Recommendation 11:** Do not amend Nova Scotia's access and privacy laws to extend time limits for responding to applicants' access requests.

**Recommendation 12:** Amend Nova Scotia's access and privacy laws to, with the permission of the Commissioner, allow public bodies to take a time extension if an applicant initiates multiple concurrent requests to the same public body and responding to them would unreasonably interfere with the public body's operations.

**Recommendation 13:** Amend Nova Scotia’s access and privacy laws to give the Commissioner the power to place review requests on hold where the applicant has five or more active reviews. Allow the Commissioner to hold additional review requests in abeyance and not commence an investigation until one of the five active complaints is resolved.

**Recommendation 14:** Implement a directive to all Nova Scotia Government department staff that responses to access requests cannot be delayed because they are waiting for sign-off.

Alternatively, amend Nova Scotia’s access and privacy laws to make clear that waiting for sign-off is not an authorized reason to delay responding to an access request.

**Recommendation 15:** Amend Nova Scotia’s access and privacy laws to make it clear that views or interests of third parties must be canvassed instead of assumed by public bodies when making disclosure decisions related to third party personal information or confidential business information.

**Recommendation 16:** Amend Nova Scotia’s access and privacy laws to better anonymize the name and type of applicant within a public body similar to s. 12 of Newfoundland and Labrador’s *Access to Information and Protection of Privacy Act*.

**Recommendation 17:** Amend Nova Scotia’s access and privacy laws to make it clear whether public bodies can or cannot withhold information based on the information being “non-responsive” by creating that authority as a limited and specific exemption. If an amendment is made to include “non-responsive” as an exemption, include a definition of this term.

**Recommendation 18:** Initiate consultation with Indigenous organizations, Indigenous governments, and other relevant stakeholders to consider whether Nova Scotia’s access and privacy laws can better reflect the needs and expectations of Indigenous people.

**Recommendation 19:** Create a definition of “Indigenous government” that would better encompass Indigenous governments and organizations in Nova Scotia.

**Recommendation 20:** Amend Nova Scotia’s access and privacy laws to state that disclosure does not amount to an unjustified invasion of personal privacy if it discloses information about a deceased individual to a spouse or a close relative of the deceased individual, and the public body is satisfied disclosure is desirable for compassionate reasons.

Alternatively, amend Nova Scotia’s access and privacy laws to include compassion as a relevant circumstance to consider when weighing whether disclosure of third party personal information would be an unreasonable invasion of their personal privacy.

**Recommendation 21:** Amend Nova Scotia’s access and privacy laws to include a definition of “use” of personal information consistent with that found in Newfoundland and Labrador’s *Personal Health Information Act*.

Alternatively, set out a definition that is consistent with Nova Scotia’s *PHIA*.

**Recommendation 22:** Amend Nova Scotia’s access and privacy laws to be consistent with international legal instruments that attempt to ensure adequate protection of young people’s privacy rights that protect them from the risks of the online world.

**Recommendation 23:** Amend Nova Scotia’s access and privacy laws to include provisions that address when an individual under the age of 19 can exercise their access and privacy rights.

**Recommendation 24:** Review whether the provisions of the *Personal Information International Disclosure Protection Act* would benefit from any amendments. Put all storage and disclosure of personal information outside of Canada provisions within one combined access and privacy law so that there will be a means for independent oversight and all storage and disclosure of personal information outside of Canada will be required to follow the same safety requirements set out in Nova Scotia’s existing access and privacy laws.

**Recommendation 25:** Canvass the privacy concerns associated with automated decision-making, AI, and generative AI, and consider whether legislative amendments are required to address this emerging technology. Consideration should be given to whether Nova Scotia’s access and privacy laws should be amended to:

- a) Incorporate definitions of automated decision-making, AI, and generative AI.
- b) Require that algorithmic assessments and privacy impact assessments be conducted prior to the implementation of any projects or programs involving the use of automated decision-making, AI, or generative AI.
  - i) Require these assessments be provided to the OIPC for comment prior to implementation.
- c) Set out “no-go zones” for the use of automated decision-making, AI, or generative AI, such as the creation of projects or programs for malicious purposes.
- d) Give individuals the right to be notified when automated decision-making technologies are being used to make decisions about them.
- e) Give individuals the right to object to the use of automated processing of their information.
- f) Require public bodies to have technology that allows them to create a traceable record of how a decision was made.
- g) Disclose the reasons and criteria used for any automated decision.

**Recommendation 26:** Amend Nova Scotia’s access and privacy laws to include a definition of “biometric information” and to set out the significant independent oversight mechanisms that this very sensitive information warrants.

**Recommendation 27:** Review data linking legislative developments in other jurisdictions and include provisions in Nova Scotia’s access and privacy laws that address the concept of data linking in terms of transparency, privacy protections, and oversight.

**Recommendation 28:** Amend Nova Scotia’s access and privacy laws to give the OIPC financial independence.

**Recommendation 29:** Amend Nova Scotia’s access and privacy laws to require that public bodies must provide transparent, intelligible, justifiable, and reasonable reasons for rejecting any of the Commissioner recommendations.

**Recommendation 30:** Explore options to enhance the decision-making powers of IAP Services’ administrators. If they are expanded, increase their compensation to reflect their expertise and job requirements.

**Recommendation 31:** Explore options to increase the compensation of OIPC staff to reflect their expertise and job requirements.

**Recommendation 32:** Amend Nova Scotia’s access and privacy laws to give the Commissioner the same general powers that are commonplace in more modern Canadian legislative schemes.

## Appendix B - Suggested readings

1. (2017 *Special Report*) Office of the Information and Privacy Commissioner for Nova Scotia, *Accountability for the Digital Age, Modernizing Nova Scotia's Access & Privacy Laws* (June 2017), online: <[https://oipc.novascotia.ca/sites/default/files/publications/annual-reports/Accountability for the Digital Age %28June 2017%29 .pdf](https://oipc.novascotia.ca/sites/default/files/publications/annual-reports/Accountability%20for%20the%20Digital%20Age%20June%202017%29.pdf)>.
2. (2021-2022 *Annual Report*) Office of the Information and Privacy Commissioner for Nova Scotia, *2021-2022 Annual Report* (October 2022), online: <[https://oipc.novascotia.ca/sites/default/files/reports/2021-2022 OIPC Annual Report.pdf](https://oipc.novascotia.ca/sites/default/files/reports/2021-2022%20OIPC%20Annual%20Report.pdf)>.
3. *BC Investigation Report P19-01, Full Disclosure: Political parties, campaign data, and voter consent*, [2019 CanLIIDocs 4376](#).
4. Centre for Law and Democracy, *Canadian RTI Rating*, online: <<https://www.law-democracy.org/live/rti-rating/canada/>>
5. Clyde Wells, Doug Letto, & Jennifer Stoddart, Newfoundland and Labrador, *Report of the 2014 Statutory Review for Access to Information and Protection of Privacy Act Newfoundland and Labrador* (March 2015), online: <[https://www.oipc.nl.ca/pdfs/ATIPPA Report Vol2.pdf](https://www.oipc.nl.ca/pdfs/ATIPPA%20Report%20Vol2.pdf)>.
6. *Cummings v. Nova Scotia (Public Prosecution Service)*, [2011 NSSC 38 \(CanLII\)](#).
7. *Daniels v. Wolfville (Town)*, [2023 NSSC 126 \(CanLII\)](#).
8. *Donham v. Nova Scotia (Information and Privacy Commissioner)*, [2023 NSSC 87 \(CanLII\)](#).
9. Federal, Provincial and Territorial Information and Privacy Commissioners *Securing Trust and Privacy in Canada's Electoral Process* (September 2018), online: <<https://oipc.novascotia.ca/sites/default/files/publications/FPT%20Resolution%202018%20%282018%20Sept%202017%29.pdf>>.
10. Federal, Provincial and Territorial Information and Privacy Commissioners *Resolution: Putting best interests of young people at the forefront of privacy and access to personal information* (2023), online: <[https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res\\_231005\\_01/](https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_01/)>.

11. Federal, Provincial and Territorial Information and Privacy Commissioners *Joint Statement: Principles for responsible, trustworthy and privacy-protective generative AI technologies* (December 7, 2023), online: <[https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd\\_principles\\_ai/#fn2](https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/#fn2)>.
12. G7 Data Protection and Privacy Authorities, *Statement on Generative AI* (June 2023), online: <[https://www.priv.gc.ca/en/opc-news/speeches/2023/s-d\\_20230621\\_g7/](https://www.priv.gc.ca/en/opc-news/speeches/2023/s-d_20230621_g7/)>.
13. G7 leaders, *G7 Leaders' Statement on the Hiroshima AI Process* (October 2023), online: <<https://www.mofa.go.jp/files/100573466.pdf>>.
14. Global Privacy Assembly, *Resolution on Generative Artificial Intelligence Systems* (2023), online: <<https://globalprivacyassembly.org/wp-content/uploads/2023/10/5.-Resolution-on-Generative-AI-Systems-101023.pdf>>.
15. Government of Canada, *Access to Information Review Indigenous-specific What We Heard Report* (August 2023), online: <<https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/reviewing-access-information/the-review-process/indigenous-specific.html>>.
16. Government of Canada, *Directive on Automated Decision-Making* (April 2019), online: <<https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>>.
17. Information Access and Privacy Services, *2022/23 Annual Report* (undated), online: Nova Scotia Government <<https://beta.novascotia.ca/sites/default/files/documents/1-2551/information-access-and-privacy-services-annual-report-en.pdf>>.
18. *Krieger v. Law Society of Alberta*, [2002 SCC 65 \(CanLII\)](#), [2002] 3 SCR 372.
19. Legislative Assembly of British Columbia, *Special Committee to Review the (BC) Freedom of Information and Protection of Privacy Act, FIPPA for the Future* (June 2022), online: <[https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/3rd-session/fippa/report/SC-FIPPA-Report\\_42-3\\_2022-06-08.pdf](https://www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/3rd-session/fippa/report/SC-FIPPA-Report_42-3_2022-06-08.pdf)>.
20. *Newfoundland and Labrador (Information and Privacy Commissioner) v Newfoundland and Labrador (Justice and Public Safety)*, [2023 NLCA 27 \(CanLII\)](#).
21. Nova Scotia House of Assembly, *Debates and Proceedings* (November 8, 1993, November 22, 1993), online: <<https://legcat.gov.ns.ca/wamvalidate?url=https%3A%2F%2F0-nsleg--edeposit-gov-ns-ca.legcat.gov.ns.ca%3A443%2Fdeposit%2FHansardDeposit%2F56-01%2F19930913.pdf>>.

22. *Nova Scotia (Public Prosecution Service) v. FitzGerald Estate*, [2015 NSCA 38 \(CanLII\)](#).
23. *NS Review Report 16-08, Nova Scotia (Department of Justice) (Re)*, [2016 NSOIPC 8 \(CanLII\)](#).
24. *NS Review Report 16-12, South Shore Regional School Board (Re)*, [2016 NSOIPC 12 \(CanLII\)](#).
25. *NS Review Report 21-09, Department of Health and Wellness (Re)*, [2021 NSOIPC 9 \(CanLII\)](#).
26. *O'Connor v. Nova Scotia*, [2001 NSCA 132 \(CanLII\)](#).
27. Office of the Information and Privacy Commissioner for British Columbia, *Submission to the Special Committee to Review the Freedom of Information and Protection of Privacy Act* (March 2022), online: <<https://www.oipc.bc.ca/legislative-submissions/3656>>.
28. Office of the Information and Privacy Commissioner for Newfoundland and Labrador, *Submission of the Information and Privacy Commissioner to David B. Orsborn, Committee Chair of the ATIPPA Statutory Review Committee 2020 on the Review of the Access to Information and Protection of Privacy Act (ATIPPA, 2015)* (2020), online: <<https://www.oipc.nl.ca/pdfs/OIPCATIPPA2015-2020StatReviewSubmission.pdf>>.
29. Office of the Information and Privacy Commissioner for Nova Scotia, *Time Extension Request Guidelines for Public Bodies* (November 2022), online: <[https://oipc.novascotia.ca/sites/default/files/forms/FOIPOP%20Forms/2022%2011%2001%20FOIPOP%20Time%20Extension%20Guidelines\\_0.pdf](https://oipc.novascotia.ca/sites/default/files/forms/FOIPOP%20Forms/2022%2011%2001%20FOIPOP%20Time%20Extension%20Guidelines_0.pdf)>.
30. Office of the Saskatchewan Information and Privacy Commissioner, *Data Matching* (May 2017), online: <<https://oipc.sk.ca/assets/data-matching.pdf>>.
31. Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent* (August 2021), online: <[https://priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl\\_omc\\_201805/](https://priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/)>.
32. Ontario Government, *Ontario Public Service Data Integration Data Standards*, (April 2021), online: Ministry of Government and Consumer Services <<https://files.ontario.ca/mgcs-ontario-public-service-data-integration-data-standards-april-2021-en-2021-04-29.pdf>>.
33. *Raymond v. Halifax Regional Municipality*, [2022 NSSC 68 \(CanLII\)](#).

34. Tim Houston, *Mandate Letter to the Minister of Justice* (September 2021), online: Nova Scotia Government <[https://novascotia.ca/exec\\_council/letters-2021/ministerial-mandate-letter-2021-AG-DOJ.pdf](https://novascotia.ca/exec_council/letters-2021/ministerial-mandate-letter-2021-AG-DOJ.pdf)>.
35. United Nations, *Convention on the Rights of the Child* (November 1989), online: <<https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>>.
36. *VinAudit Canada Inc v Yukon (Government of)*, [2023 YKSC 68 \(CanLII\)](#).