OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
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)

November 25, 2020

Table of Contents

Introduction

The Report of the 2014 Statutory Review of the *Access to Information and Protection of Privacy Act*, including the bill that was drafted as part of that process, is a landmark achievement in the development of access to information and protection of privacy law in Canada. The resulting law, our current *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015)* has been recognized nationally and internationally for the ways in which it thoughtfully threaded the needle of balancing important rights set out in the *Act* with the necessary exceptions to those rights. For privacy, this means a statutory regime that recognizes and codifies the right of privacy while setting out those collections, uses, and disclosures which are necessary for public bodies to function and serve the public. For access to information, this involved extensive research and analysis of the right of access and the exceptions to that right, to ensure that the exceptions protect only those interests that need to be protected, and no more.

Most reviews of public sector access and privacy laws will not have the resources or mandate given to the 2014 review, nor will the particular political climate of that time likely be present during such reviews. That being said, like tuning a fine instrument, each review is an opportunity to ensure that the balance established in *ATIPPA, 2015* remains harmonious.

Our highest priority is to see the current provisions of *ATIPPA, 2015* largely continue as they are. If nothing at all were to change in *ATIPPA, 2015*, it would remain at or near the top of public sector access and privacy statutes in Canada. The worst possible outcome, however, would be one which sees access or privacy rights, or oversight thereof, deteriorate in any way. As an Office dedicated to oversight of this statute, we believe there are only a select few necessary changes to *ATIPPA, 2015*, none of which should impact the overall harmony of the *Act*, but rather support the vision behind *ATIPPA, 2015*.

At the outset, we would like to draw attention to three key issues that substantially impact the proper functioning of the *Act*. One relates to the ability of the Commissioner to access and review all public body records during the investigation of a complaint, including records subject to a claim of solicitor-client privilege. Our past experience with this issue shows that public bodies may be tempted to claim this privilege in questionable circumstances when independent review of that decision is only to be found in the intimidating and potentially expensive legal arena, rather than accessible to access to information applicants through the Commissioner. The other priority for review and potential amendment is section 33 (workplace investigations), a unique and potentially valuable provision, although in need of a serious tune-up. Finally, we have recommendations to legislate a duty to document which, in our view, is a natural counterpart to access-to-information legislation that ensures that public bodies record their important decisions so that the public can have access to information about them. This was a recommendation of the 2014 Statutory Review Committee that was not implemented. It has since been recommended by Commissioner Richard LeBlanc following the Muskrat Falls Inquiry. We support these recommendations and have specific comments about how to entrench a duty to document in law.

We also believe that the time is right to modestly expand the scope of the *Act*. While the political context surrounding the 2014 statutory review surrounded access to information, and the most progressive elements of *ATIPPA, 2015* are related to access, at the present there is a growing level of attention to privacy. The greatest level of attention, domestically and internationally, has been in relation to the private sector as people around the world have become increasingly wary about the extent to which

private companies large and small are collecting, using, and disclosing our personal information. This has led to major new legislation in Europe (the *General Data Protection Regulation*), the United States (the *California Consumer Privacy Act*) and now in Canada (C-11, recently introduced into the House of Commons, and Bill 64, recently introduced into Quebec's National Assembly). Each of these enactments do or would strengthen privacy rights and oversight vis-à-vis the private sector. The jurisdiction of *ATIPPA, 2015* in this province is the public sector, and we believe that residents have even higher expectations about the level of care taken by public bodies who hold their information than private companies. This has been illustrated in recent months as the public has responded to the launch, in most Canadian jurisdictions, of the COVID Alert app. Notwithstanding the critical public health imperative, and assurances of its privacy protections from experts, Commissioners, and others, many were still reluctant to download an app that they perceived to involve a government tracking where they went and who they came into contact with. Many even took to social media, which of course does these very things, to express these viewpoints. We can understand this reaction: even though the private sector is so pervasive, our public bodies do have monopoly control over most of the services that they provide, and the authority of the law behind their decision-making. In many instances, citizens and residents really do have no choice but to provide their personal information. We think the time is right for our public sector privacy legislation to take steps to keep pace with these developments.

We have a number of modest proposals to align the privacy protections in *ATIPPA, 2015* with those in *PHIA*, such as requiring public bodies to develop information policies, introduce oaths of confidentiality for officials who handle personal information, and allow for privacy breach complaints to be made to the OIPC on a prospective basis. We also recommend, as Federal, Provincial, and Territorial Privacy Commissioners have jointly called for, that we include political parties within the scope of the *Act*. Though we do not believe that these organizations should be treated as public bodies for all of the purposes of the *Act*, we are of the view that there should be some regulatory oversight of how these organizations handle personal information. Finally, as public bodies expand their digital services, some public bodies may begin to introduce certain technologies that are not, in our view, adequately regulated by our current legislation. We propose modest first steps to help prepare us for the increasing interest in the collection of biometric information by public bodies and the introduction of artificial intelligence into digital services. With government's firm commitment to transform its service delivery model to the digital realm, the challenge of doing so in a way that respects privacy is one that is already upon us. We need to ensure that our statute is crafted in such a way that these innovations are possible, while at the same time ensuring that the fundamental rights at play are protected.

Beyond these, many of our recommendations are focused on ways to ensure that the intentions of the 2014 ATIPPA Review Committee are more fully realized. Some of these may be relatively minor in nature, but they will improve the clarity and user-friendliness of the *Act*.

The bulk of the remainder of this document focuses upon the above-referenced recommendations. Appendix A provides a consolidated list of them for ease of reference; however, at this juncture we wish to make some additional comments on the legislative review.

Any review of an access or privacy statute will elicit feedback from those who suggest that the provisions have in some sense gone too far. In particular, we expect you to hear, from some, that the access provisions are too liberal and unreasonably interfere with the operations of the public body by exposing

information that should be kept confidential or taxing the scarce resources of overworked ATIPP Coordinators, executive and other government officials. We have certainly heard our share of complaints about the workload and challenges presented by the statute, and those are real. In our view these are primarily challenges of implementation, rather than issues with the statute itself. Since *ATIPPA, 2015* the number of access requests to public bodies has increased annually. This is a mark of success, because it demonstrates that the general public are aware of their rights and availing of them. This vibrancy supports transparency of public bodies and democratic accountability. The Green Report and the Muskrat Falls Inquiry tell us something about what happens when those values are lacking in our statutory framework.

That being said, the simple fact is that access requests require work on the part of public bodies, and the more requests there are, the more work that needs to be done. It is important to recognize, however, that short of a massive curtailing of access to information rights, statutory amendments will not address those problems for the most part. Raising or adding costs or fees simply creates another administrative task for public bodies. Broadening exceptions does not reduce the workload of processing requests; however it might increase the number of complaints, which will add to the workload. Eroding oversight will also not reduce the number of requests; however it will reduce trust in our public institutions at a time when that trust is already under attack from all directions. Instead, we believe that there are some administrative solutions that might address some of the issues that are causing stress and anxiety to the Coordinators who work at the coalface of *ATIPPA, 2015*.

The Report of the 2014 Statutory Review of *ATIPPA* devoted substantial attention to the role of Coordinator. While there have been significant improvements in terms of respect for that role within public bodies, one of the key suggestions that came forth was that Coordinators in core government be situated at a Director level. That was not a formal recommendation, and while we understand it was considered, it was not implemented. That being said, we believe it would be a good idea to explore options to enhance the authority and compensation level of Coordinators. This is important not only to ensure respect for the role and to ensure sufficient autonomy within the organization, but we believe it is important to recognize the important work of Coordinators and to retain skilled Coordinators in their jobs. In our view, it would be a mistake to simply transfer the Coordinator role to an existing Director who already likely has more than a full plate. Instead, Coordinator roles should be recognized for the challenging positions that they are. The Coordinator role demands a high degree of expertise in access to information, but there should also be greater recognition of their role in helping to implement and advise on the privacy responsibilities of public bodies. Employees occupying these roles interact with senior executive within their public bodies in what can be a stressful context. Finding ways to reflect that by redefining those roles and improving compensation would assist in attracting and retaining individuals with the necessary expertise.

Within core government there is an established process whereby if a public body receives an access request which touches on the work of another public body, there must be a consultation between those public bodies. This drives a significant amount of work for Coordinators. In some cases the consultation is necessary, however we have heard anecdotally of situations whereby this may be occurring more than necessary, adding to the workload of the ATIPP system. Included in this is the requirement in government policy to notify Executive Council whenever it is believed that responsive records could fall under the cabinet exception at section 27. The Chair may wish to inquire into the consultation process, including the

process of consulting with Executive Council, to determine whether efficiencies may be identified that could reduce workload stress within the system.

The statutory deadlines within the *Act* are often pointed to as a source of stress. We believe the extension and disregard processes set out in *ATIPPA, 2015* are largely successful as breakers for system overload. The OIPC has a fairly consistent record of approving, either in full or in part, 90% of extension requests that come to us. The partial approvals, as well as the few rejections, demonstrate that we aim to ensure that access to information applicants are not unduly impacted when delays cannot reasonably be justified. When it comes to the disregard process, our approval rating is lower, however the bar for approval is higher – appropriately so, given that this amounts to the abrogation of a right. The statistics do not tell the whole story, however. Some requests for disregard are ultimately withdrawn. Sometimes, either through the Coordinator's own efforts, or with our assistance, the Applicant comes to understand that a more specific or reasonable request will serve their intended purpose and will avoid being subject to a disregard. That being said, one of the challenges with section 23 is that Coordinators must be in a position to assess the scope and scale of the request, contact the applicant and, most importantly, actually reach the Applicant, before deciding that an application for approval to disregard must be made. Unfortunately for Coordinators, this must all occur within 5 business days in accordance with section 21, which places them in an extremely difficult position at times. It is our view that the rights of applicants will not be unduly interfered with if that deadline became 10 business days. (See Recommendation 16.6.) In fact, this adjustment could benefit applicants, because if the Coordinator is not able to reach the Applicant by business day 5 for a request that the Applicant may not realize is an unreasonable request, the result could be that the request receives approval to be disregarded. The Applicant may then assume that access to information is a dead end and not bother to apply again with a more targeted request.

Also, we have noted the mandate that the Chair was provided with at the commencement of the Statutory Review and wish to make a number of comments about certain subjects within it. To that end, for your convenience, in Appendix B we have broken down the mandate into its components and offer comments after each one and in certain instances direct the Chair to the recommendations in the body of the submission that speak to that aspect of the mandate.

As a final introductory note, we respectfully ask you to recommend that the OIPC be consulted on the timeframe for proclamation of any amendments that may result from this review and, if different, the date that it will be brought into force. We ask this so that we can prepare new training and/or resources that may be required to prepare public bodies and/or our Office to work with the new *Act*.

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

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

> *3. (1) The purpose of this Act is to facilitate democracy through*
>
> > *(a) ensuring that citizens have the information required to participate meaningfully in the democratic process;*

> *(b) increasing transparency in government and public bodies so that elected officials, officers and employees of public bodies remain accountable; and*
>
> *[…]*
>
> *(2) The purpose is to be achieved by*
>
> *[…]*
>
> *(f) providing for an oversight agency that*
>
> *[…]*
>
> *(iii) provides independent review of decisions made by public bodies under this Act,*

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

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

No sooner had the Court of Appeal issued its judgment, the Government of Newfoundland and Labrador, upon completion of the first statutory review of *ATIPPA*, amended the *ATIPPA* to remove the authority and mandate of the Commissioner to review claims of solicitor-client privilege in the course of an access to information review investigation. That amendment was part of Bill 29, which was roundly condemned in the public discourse of the day as having the effect of impairing the Commissioner's ability to perform his function, because he was unable to independently verify the claims of public bodies when reviewing of their decisions to deny access to information. Under the Bill 29 version of the *Act*, the only route available for independent review for such denials of access was through the time-consuming, resource-intensive, and costly court process. The removal of the first level of independent review by the Commissioner placed an unnecessary burden upon the Courts and impacted the purposes of the *Act*, as access delayed is often access denied.

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

> *Most participants who commented on solicitor-client privilege felt that the Commissioner must be able to read all documents, including solicitor-client privileged documents and documents involving Cabinet confidences. They expressed the view that the statutory provision as it existed before Bill 29 should be restored. In discussions with the Committee, participants often argued*

that the reason the Commissioner should be able to examine documents subject to a claim of solicitor-client privilege is that otherwise the Commissioner will be unable to perform his duties properly. That is also the basis on which Justice Harrington concluded (above) that it was "absolutely necessary" for the Commissioner to be able to compel production of solicitor-client privileged documents.

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

The Committee recommends that

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

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

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

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

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

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

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

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

The above recommendations were accepted by government, and in fact the House of Assembly voted unanimously to accept (with two minor, unrelated amendments) the draft Bill developed by the Committee, which included specific language intended to fulfil those recommendations. After the coming

into force of the *ATIPPA, 2015* the OIPC resumed its former practice of reviewing claims of solicitor-client privilege, which often, but not always, involved obtaining a copy of the records for that purpose from the public body. After the review is over, all records obtained from a public body are subject to the OIPC's records destruction protocol that is strictly observed.

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

JPS indicated that its new position on the Commissioner's authority to compel production of and review claims of solicitor-client privilege resulted from the issuance of a decision by the Supreme Court of Canada in *Alberta (Information and Privacy Commissioner) v. University of Calgary 2016 SCC 53*. JPS appears to have waited for two years after that ruling for the right opportunity to take this position. While we appreciate that governments must ensure that its statutes are not in conflict with Supreme Court of Canada rulings, the course of action taken by JPS, particularly given the history of this issue in this province, is puzzling. Our view is that the statutory language in *ATIPPA, 2015* clearly gives the OIPC the authority to review claims of solicitor-client privilege. Their position is that it does not.

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

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

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

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

> *97(5) The head of a public body may require the commissioner to examine the original record at a site determined by the head where*
>
> > *(a) the head of the public body has a reasonable basis for concern about the security of a record that is subject to solicitor and client privilege or litigation privilege;*
>
> *(6) The head of a public body shall not place a condition on the ability of the commissioner to access or examine a record required under this section, other than that provided in subsection (5).*
>
> *100 (2) The solicitor and client privilege or litigation privilege of the records shall not be affected by production to the commissioner.*

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

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

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

> *Mr. Speaker, government is introducing a blanket exemption on the release of any information touching upon solicitor-client privilege; any appeal must be done through the Supreme Court rather than through the Privacy Commissioner.*
>
> *Mr. Speaker, why is government forcing people of this Province into expensive and lengthy legal court action on matters which could easily be avoided by referring to the Privacy Commissioner?*
>
> *[…]*
>
> *I referred earlier, Mr. Speaker, to a Supreme Court, Court of Appeal decision. It was a case between the Information and Privacy Commissioner. This was an appeal of a decision at the*

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

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

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

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

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

With *ATIPPA, 2015*, a clear policy choice was made by the Legislature after a thorough analysis of the issues canvassed by the 2014 Statutory Review Committee, and explicitly stated as such by the Minister when introducing the new Act in the Legislature. Even if the present government legitimately harbours some doubt, in light of the University of Calgary decision, whether the statutory language in *ATIPPA, 2015* is entirely sufficient for its intended purpose, there were two choices before it. It could have introduced an amendment in the legislature to add additional language for greater certainty. For reasons unknown to the OIPC, it chose instead to simply refuse to provide records to the Commissioner for review where there was a claim of solicitor-client privilege. In doing so, it opened up another era of uncertainty, whereby some public bodies are following suit and others not, creating an unnecessary standoff which will see matters continue to clog up the court system, for the benefit of whom? This has been a baffling and frustrating experience for the OIPC as well as access to information requesters who must now wait an

indefinite period of time for their matters to be resolved. In terms of the effect on requesters, our Report A-2013-004, particularly paragraphs 36 through 40, illustrates the path that these matters can take when there is no opportunity for review by the Commissioner.

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

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

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

> *36 (2.1) The Information Commissioner may examine a record that contains information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege only if the head of a government institution refuses to disclose the record under section 23.*
>
> *(2.2) For greater certainty, the disclosure by the head of a government institution to the Information Commissioner of a record that contains information that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege does not constitute a waiver of those privileges or that professional secrecy.*

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

Our recommendation to the Chair of this Review is that an amendment to the *ATIPPA, 2015* is required, not because the current statutory language is insufficient, but simply to bring an end to what has been a seemingly endless campaign, irrespective of political stripe, of governments of this Province wishing to impair the ability of the Commissioner to discharge his role as derived from the purpose of the *ATIPPA, 2015*. Such an amendment would re-affirm, once and for all, the policy choice that was adopted by the Legislature in 2015, and supported by the current Attorney General by his vote in favour of the new statute, as well as in debate over Bill 29 in 2012. The current legislation contains the necessary safeguards

to protect solicitor-client privilege upon disclosure to the Commissioner, and public bodies always have the right to ask the Court to review the matter following an assessment by the Commissioner. The challenge to this first level of independent review is unnecessary and contrary to meaningful access to information.

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

Workplace Investigations

Section 33 has been a challenge for public bodies and access to information applicants, as well as for those other parties to a workplace investigation whose information has been accessed through this unique provision. It has also challenged this Office in overseeing compliance. We have created a guidance document and issued several reports pertaining to this section, however we can also see that there may be circumstances where what we believe to be the correct interpretation is one that could have unintended negative consequences, as the Commissioner noted at paragraph 14 of Report A-2020-024. Although the recommendations below may be viewed, on balance, as representing a restriction on the right of access, it is important to recognize that as stewards of the *Act*, we have an equal role (as recognized in section 3(2)(f)) in promoting both access to information and protection of privacy. This submission on section 33 is simply our effort to help find the appropriate balance between those competing values.

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

While the OIPC supports the principle of a right of access of a party to a workplace investigation to certain information relevant to the investigation, the breadth of this right in scope and time in the current statute has, we believe, created a number of likely unintended consequences. We therefore have three recommendations, discussed in turn below:

Precedence of Section 33 Over Other Exceptions

This provision first appeared with the Bill 29 amendments to the *ATIPPA* in 2012, when it became section 22.2 of that *Act*. It was subsequently amended following the Wells Review at our suggestion, replacing the phrase "the substance of records collected or made during a workplace investigation" with "all relevant information created or gathered for the purpose of a workplace investigation" to provide greater

clarity. The Cummings Legislative Review Report featured some discussion of workplace investigations, but did not specifically recommend the approach that was ultimately taken in the Bill. Anecdotally, our observation is that in the years prior to the inclusion of section 22.2 (now section 33) that public bodies found it particularly challenging to process requests for access to information from parties involved in workplace investigations.

In particular, a request for access to one's own personal information that was collected or gathered as part of a workplace investigation (whether filed by the complainant or respondent) would typically result in a set of responsive records including things such as the statements of the parties, witness statements, investigator's notes, comments or discussions in emails between parties or among HR officials about the investigation, etc. Various exceptions to the right of access may have been applied to some of this material, but ultimately individuals have a right of access to their own personal information, including the opinions of others about them. Access and Privacy Coordinators found it particularly difficult at times to untangle, within these types of records, whether information was the personal information of one party or another, which led to inconsistent redaction and frequent complaints to the OIPC. This is our perspective on the genesis of why we have a section 33, although we cannot claim any inside knowledge in terms of any discussions which may have been had or rationales debated among government officials leading up to the time the original version of section 33 first appeared.

Despite the fact that this provision first appeared in the *ATIPPA* in 2012, it was not until 2016 that the OIPC was called upon to interpret it in a formal report. Since then, however, it has appeared frequently, having been addressed or discussed in the following Reports:

- A-2016-023 – City of Corner Brook
- A-2018-017 – City of Corner Brook
- A-2019-004 – Commissioner for Legislative Standards
- A-2020-001 – College of the North Atlantic
- P-2020-001 – City of Mount Pearl
- A-2020-013 – City of Mount Pearl
- A-2020-015 – Memorial University
- A-2020-024 – Human Resource Secretariat

Report A-2018-017 was the subject of an application for a declaration by the City of Corner Brook under section 50, in which Justice Handrigan determined at paragraph 87 that the subject matter of the records was not in fact a workplace investigation, but an investigation for a different purpose:

> *Overall, I am satisfied that the City Solicitor's investigation and report to City Council was not a workplace investigation. It was first and foremost a rigorous assessment of the liabilities that the City might have to [complainant] because of his threatened legal actions.*
>
> *Corner Brook (City) v. Newfoundland and Labrador (Information and Privacy Commissioner), 2020 NLSC 37*

Report A-2019-004 resulted in an appeal being filed by the access to information Applicant. Among the findings in that Report were that a Member of the House of Assembly is not an employee as defined in

ATIPPA, 2015, and therefore is not able to avail of section 33, owing to the language in section 33(1)(c). The matter has been heard and a decision is pending at this time.

Reports A-2020-001 and A-2020-015 are subject to applications for a declaration by the College of the North Atlantic and Memorial University respectively. Neither matter has yet been heard. Reports P-2020-001 and A-2020-013 involving the City of Mount Pearl should be read in sequence, as both relate to records from the same workplace investigation; however, it is Report A-2020-013 which directly addresses section 33.

As noted above, our experience is that section 33 has continued to pose challenges for all involved, including this Office. We are concerned that our efforts to interpret the statute consistently could result in unintended negative consequences for some affected parties. For those reasons, we believe it is important that it receive close attention during this legislative review.

If our understanding of the purpose of section 33 is correct, i.e. to provide a greater right of access to the parties to a workplace investigation than would have been provided prior to the inclusion of this provision in the statute, its intent must be to override section 40, to avoid circumstances where the personal information of the applicant was *also* the personal information of another person, and to ensure the applicant received all relevant information. Otherwise there would be no purpose for section 33 and the ordinary right of access to one's own personal information would provide all the access to information to which the applicant is entitled. However, there is no specific reference in the statute that would identify section 40 or any other section of the statute as the sections to be overridden. Logically, therefore, section 33 must be interpreted to override all exceptions in the *A*ct. If section 40 was a discretionary exception, then perhaps a logic might be considered whereby the class of discretionary exceptions could be overridden, but not the mandatory exceptions; but this is not the case. This leaves us in a precarious and uncertain place, as there are certain exceptions which perhaps should take precedence over section 33.

Consider the case that gave rise to A-2020-024. In this case, the public body withheld the names and identifying information of the witnesses, citing section 37(1)(a), because it claimed there was a likelihood of harm to the witnesses should that information be released. A similar claim was made by a different public body and was the subject of A-2020-001. In both cases, the Commissioner found that the public bodies had not presented any evidence to substantiate their allegations of harm and therefore the public bodies had not satisfied their burden of proof that section 37 applied to this information; however, these findings were incidental to the recommendations of these reports: that section 33 prevails over section 37[1]. The implication was that even if there was evidence of a risk to harm, then the applicant would still have had a right of access to the information.

> **<u>Recommendation 2.1:</u> Amend section 33 to provide that certain other exceptions in the *Act* are to be applied to the records before any disclosure, regardless of section 33. Chief among those would be section 27 (cabinet confidences), section 30 (legal advice), section 31 (law enforcement) and section 37(1)(a) (individual or public safety).**

[1] In the case of A-2020-001, the public body has filed an application with the Supreme Court for a Declaration that it does not have to follow the Commissioner's recommendation; in the case of A-2020-024 the public body has accepted the recommendation and released the relevant information to the complainant.

Limit Temporal Aspect of Section 33 Applicability

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

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

What section 33 does not reflect is that harassment typically involves a power relationship between the perpetrator or abuser and the subordinate victim. Harassment is only possible because of that inequality.[2] The power relationship also means that harassment is easily accompanied by intimidation of the victim, and a complaint can easily result in retaliation. It is only because of that inequality that specific respectful workplace policies, and specific workplace investigation processes, are necessary.

There are in Canada a number of practitioners who specialize in workplace investigations, and there is a professional literature on the conduct of such investigations[3]. In that literature, and in many respectful workplace policies, it is recognized that because of the inequality in power relationships, harassment complainants and witnesses need assurances of confidentiality. Otherwise the fear of intimidation and retaliation will prevent them from coming forward. The investigator needs to be able to provide assurances of confidentiality in order to build a relationship of trust with the complainant and witnesses, and to ensure complete disclosure during the investigatory process.

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

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

In typical investigations, the investigator has a mandate to provide a report to the employer containing a statement of facts, summarizing the information provided by witnesses, without any recommendation for

[2] It may be noted that there are instances of co-worker harassment, but that involves a different kind of power relationship. It may also be noted that most abusers are male, for example. But that does not affect the problems created by s.33.

[3] See e.g. Rubin and Thomlinson, *Human Resources Guide to Workplace Investigations*, 2nd ed., 2018, and their firm's website.

action. Witness statements may or may not be provided to the employer, or to the respondent, and may be summarized, de-identified or redacted. All of these considerations should, ideally, be reflected in policies and procedures. The reality, however, is that there is a broad range of resources and expertise between the smallest municipality and the largest government department, so this may not always be the case.

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

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

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

The legal right to full disclosure of evidence, and the identity of an accuser, exists in relation to an adjudicative process in which there can be a binding decision affecting a respondent’s legal rights. A workplace investigation is not an adjudicative process. It is analogous to a police investigation that might lead to criminal charges, or an employer’s investigation into misconduct that could lead to discipline. At the investigation stage, policy or practice often dictates that a respondent must be notified of an investigation, but there is no legal requirement that this be done, much less to engage the respondent to participate. *ATIPPA, 2015* recognizes this distinction, for example, in section 5(1)(k), in which the *Act* does not apply to law enforcement records where the investigation has not been completed.

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

respondents in harassment complaints are usually the parties who will make access requests under that section.

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

Therefore, we recommend that Government amend section 33 to provide that disclosures of workplace investigation records in response to an access request are only to be made after the workplace investigation has been completed, but before any resulting discipline is imposed or corrective action is taken by the employer. This would permit the investigator to retain control of the investigation, to explain any limits on confidentiality to witnesses, and to control when, and in what detail, the respondent is given information during the investigation process. It would also prevent a party from disrupting the investigation with an access request while the investigation is ongoing. It would furthermore assist the investigator or the public body (or the OIPC in a complaint investigation) in determining "relevance" after the investigation is complete. Furthermore, in accordance with records retention and destruction policies that may be approved under the appropriate statute or bylaws, if a complaint is withdrawn before completion, a public body could create a policy to destroy any records created or gathered by the investigator. Moreover, records of statements provided orally or in writing by a witness or complainant, or the identity of same, could be withheld until the conclusion of the investigation, unless explicit consent to disclosure is given by the individual. All parties could retain the right of access to their own statements at any time. If a temporal limitation was placed on the right of access as proposed, it would also allow for the appropriate and legally authorized destruction of any transitory records prior to an access request being allowed, such as investigators notes or audio recordings.

> **<u>Recommendation 2.2</u>: Consider amending section 33 to limit disclosure of records relating to a workplace investigation such that the right of access would commence *after* a workplace investigation has been completed, *before* any resulting discipline is imposed or corrective action is taken. The right of access would be enduring thereafter.**

Public Sector Contexts Other Than Employment Relationship

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

body. It is not entirely clear why the parties to such a harassment investigation would have different rights to access than those involved in a workplace investigation.

If section 33 was expanded to include harassment investigations in such contexts, then care should be taken to ensure that the way it overrides other exceptions to access operates correctly.

> **<u>Recommendation 2.3</u>: Consult with public bodies on whether section 33 should be broadened to apply to harassment investigations beyond the employment context.**

Duty to Document

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

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

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

Commissioner Michael Harvey's letter to Commissioner LeBlanc regarding Duty to Document is included as an Appendix C to this submission, and we will therefore avoid repeating in detail much of the content of that letter.

It is our understanding that the background work on this subject has been under way to since the Report of the 2014 Statutory Review of *ATIPPA* was issued and is largely complete. That Report recommended implementation of a Duty to Document, as an amendment to the *Management of Information Act* (*MOIA*), with compliance to be overseen by the Information and Privacy Commissioner. As with the Muskrat Falls Report, Government accepted the recommendation to implement a Duty to Document from the Report of the 2014 Statutory Review of *ATIPPA* as well but, unlike most other recommendations, decided not to immediately act upon it.

At present, *ATIPPA, 2015* applies to records in the custody or control of a public body, but it makes no comment on how public bodies document their day-to-day activities or decisions.

The closest that *ATIPPA, 2015* comes to requiring a public body to record information and maintain records is at section 63 (accuracy of personal information): "Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete." Other than this provision, *ATIPPA, 2015* is silent on the Duty to Document.

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

> *21.1 The commission, officers and staff of the House of Assembly service shall be responsible and accountable for ensuring that all advice, deliberations, decisions and recommendations of the commission that result from formal or informal meetings of the members of the commission are properly documented in accordance with the Records Management Policy of the House of Assembly.*
>
> *[…]*
>
> *66. (1) A person who fails to comply with section 21.1 is guilty of an offence.*
>
> *(2) A person having a duty to document decisions and maintain records of the commission, the speaker, the clerk or staff member of the House of Assembly service and a person who without lawful authority destroys documentation recording decisions of the commission, the speaker or the clerk, or the advice and deliberations leading up to those decisions, is guilty of an offence.*
>
> *(3) A person who is guilty of an offence under subsection (1) or (2) is liable on summary conviction to a fine of not more than $10,000 or to imprisonment up to 6 months.*

These new provisions were added as a result of a Report of the Members' Compensation Review Committee from November 2016. In addition to reporting on MHA compensation, that report identified a number of shortcomings in the operation of the House of Assembly Management Commission, and among other things it made recommendations regarding documentation of decisions and public disclosure (beginning at page 102 of that Report). In recommending the above-noted amendments, the Report also proposed that the function of the Audit Committee of the Management Commission be expanded to review compliance with these provisions. We are not aware of the extent to which this may have been implemented and if so, how well that process is functioning.

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

In 2017, British Columbia legislated a Duty to Document by adding the following to its *Information Management Act*:

> *(1) The chief records officer may issue directives and guidelines to a government body in relation to a matter under this Act, including, without limitation, the following:*
>
> *(a) the digitizing and archiving of government information;*
>
> *(b) the effective management of information by the government body;*
>
> *(c) the creation of records respecting the government information referred to in section 19 (1.1) [responsibility of head of government body], including, without*

limitation, directives and guidelines respecting the types of records that constitute an adequate record of a government body's decisions.

[. . .]

The chief records officer may do the following:

(a) access information, including personal information, held by a government body;

(b) require from an officer or employee of a government body information and explanations necessary for the chief records officer to carry out his or her mandate.

[. . .]

The chief records officer must provide to the minister an annual report on the carrying out of the chief records officer's mandate, and the minister must lay the report before the Legislative Assembly as soon as possible.

[. . .]

(1.1) Without limiting subsection (1), the head of a government body is responsible for ensuring that an appropriate system is in place within the government body for creating and maintaining, in accordance with applicable directives or guidelines issued under section 6 (1) [directives and guidelines], government information that is an adequate record of that government body's decisions. , and

(2) The head of a government body must take reasonable steps to ensure that the government body

(a) complies with directives issued under section 6 (1), and

(b) is guided by guidelines issued under that section.

Missing from the Newfoundland and Labrador *Management of Information Act* are British Columbia's provisions for "ensuring that an appropriate system is in place within the government body for creating and maintaining, in accordance with applicable directives or guidelines issued under section 6(1) [directives and guidelines], government information that is an adequate record of that government body's decisions". Although this provision in British Columbia was considered to be a step forward in the Duty to Document, the major flaw that was noted by critics at its introduction was the lack of independent oversight, as the Chief Information Officer does not report to the legislature.

The OIPC's position is consistent with the recommendation of the 2014 Statutory Review Committee, that a Duty to Document requirement should be added, ideally to the *Management of Information Act*. While we understand that the mandate of the 2020 review of *ATIPPA, 2015* is tied to that statute, we also understand that the Chair has been asked to consider the implementation of Commissioner LeBlanc's recommendation regarding Duty to Document. Therefore, we are recommending that the 2020 Committee recommend that an amendment to *MOIA* be introduced alongside the amendments to *ATIPPA, 2015*.

Moreover, we recommend that in this province, the OIPC be given oversight authority related to Duty to Document.

Recommendation 3.1: Amend the *Management of Information Act* to legislate a Duty to Document for entities subject to that legislation, providing for OIPC oversight. Consider whether to broaden the scope of public bodies to which the Duty to Document would apply, to all public bodies subject to *ATIPPA, 2015* except those that are subject to the *Municipalities Act, 1999*.

Improving Privacy Protection

Division 1, Part III of *ATIPPA, 2015* contains the statutory direction to public bodies regarding the collection, use and disclosure of personal information. This Division of the *Act* would benefit from augmentation and further clarity in order to better protect the personal information of Newfoundlanders and Labradorians. Fortunately, we need not reinvent the wheel – we can look to other statutes, including the *Personal Health Information Act* (*PHIA*) in our own province for guidance.

Information Policies and Procedures

The Information Practices section of *PHIA*, section 13, requires custodians of personal health information to "establish and implement information policies and procedures" to facilitate compliance with the *Act*. A requirement to have all public bodies implement information policies and procedures would go a long way to codifying the requirement in section 64 to take "reasonable steps" to protect information held by a public body. Written policies and procedures would help public bodies clearly communicate best practices to their staff to help prevent breaches of privacy. Based in *ATIPPA, 2015*, such policies could address: protecting confidentiality, restricting access to information by employees to those who need it to perform their duties, and providing for the secure storage, retention and disposal of personal information. Such policies could reflect what is "reasonable in the circumstances" in accordance with section 64, and having a requirement for written policies and procedures would cause heads of public bodies to turn their attention to the issue of privacy. Furthermore, with clearer expectations we believe that compliance issues are likely to be fewer.

Regarding potentially requiring policies for retention and disposal of records, it should be borne in mind that the *Management of Information Act (MOIA)* contains a restrictive definition of "public body" such that while it applies to a number of public bodies subject to *ATIPPA, 2015*, it does not apply to many other public bodies, including municipalities, educational bodies or health care bodies. Furthermore, having such a requirement in *ATIPPA, 2015* would not necessarily create a conflict, because a public body that is compliant with the requirements of *MOIA* would also be in compliance with a similar provision in *ATIPPA, 2015* if similar language is chosen.

Keeping the public informed of the policies and procedures of the public body would build confidence in the security of personal information in the custody or control of public bodies. A requirement similar to that in section 19 of *PHIA* for public bodies to make available a general description of the public body's information policies and procedures, and to provide contact information to ask questions and obtain information about how to make a complaint would achieve this goal. The OIPC has already developed a resource for public bodies about how to establish appropriate privacy policies as part of our step-by-step Privacy Management Program guidance.

Recommendation 4.1: Add a requirement to Part III, Division 1 of the *Act* for public bodies to develop information policies and procedures and to make them public.

Oaths or Affirmations of Confidentiality

Section 14 of *PHIA* could also be adapted for a revised *ATIPPA, 2015* to require the signing of oaths or affirmations of confidentiality by all staff who have contact with personal information. This would again raise awareness amongst employees and hopefully improve information handling. This obligation could be extended to contractors of the public body who may also have access to personal information.

Recommendation 4.2: Add a requirement for the swearing of an oath or affirmation of confidentiality by staff of a public body who have contact with personal information.

Definition of Consent

The option of using consent to collect, use or disclose information is present throughout *ATIPPA, 2015*, however the *Act* does not define that term. Section 23 of *PHIA* defines consent and describes how it should be obtained in order for consent to be meaningful. Any such definition of consent considered for an amendment to *ATIPPA, 2015* should be limited to circumstances involving the collection, use or disclosure of personal information, as consent in provisions such as section 34(2) (Intergovernmental Relations) or 39(2)(a) (Business Interests of a Third Party) does not have the same characteristics, nor the same requirements.

Recommendation 4.3: Include a definition of consent in *ATIPPA, 2015* modelled on the definition within *PHIA* but limited to circumstances involving the collection, use or disclosure of personal information.

Whistleblower Protection

Whistleblower protection would be an asset to *ATIPPA, 2015* as it would support individuals who act to protect personal information from collection, use or disclosure contrary to the *Act*. While the *Public Interest Disclosure and Whistleblower Protection Act* applies to some public bodies that are subject to *ATIPPA, 2015*, it only protects those who disclose offences, dangers to life, health or safety, and gross mismanagement, and that *Act* does not apply to all public bodies subject to *ATIPPA, 2015*. There should be some protection afforded to public body employees who wish to report privacy breaches or other breaches of *ATIPPA, 2015*. Section 30.3 of British Columbia's *Freedom of Information and Protection of Privacy Act* protects whistleblowers who act in good faith to protect privacy:

> *30.3 An employer, whether or not a public body, must not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee of the employer, or deny that employee a benefit, because*
>
> > *(a) the employee, acting in good faith and on the basis of reasonable belief, has notified the minister responsible for this Act under section 30.2,*

(b) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the commissioner that the employer or any other person has contravened or is about to contravene this Act,

(c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order to avoid having any person contravene this Act,

(d) the employee, acting in good faith and on the basis of reasonable belief, has refused to do or stated an intention of refusing to do anything that is in contravention of this Act, or

(e) the employer believes that an employee will do anything described in paragraph (a), (b), (c) or (d).

Similar protections are currently found in the federal private sector privacy statute, the *Personal Information Protection and Electronic Documents Act (PIPEDA):*

27 (1) Any person who has reasonable grounds to believe that a person has contravened or intends to contravene a provision of Division 1 or 1.1 may notify the Commissioner of the particulars of the matter and may request that their identity be kept confidential with respect to the notification.

Confidentiality

(2) The Commissioner shall keep confidential the identity of a person who has notified the Commissioner under subsection (1) and to whom an assurance of confidentiality has been provided by the Commissioner.

Prohibition

27.1 (1) No employer shall dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee, or deny an employee a benefit of employment, by reason that

(a) the employee, acting in good faith and on the basis of reasonable belief, has disclosed to the Commissioner that the employer or any other person has contravened or intends to contravene a provision of Division 1 or 1.1;
(b) the employee, acting in good faith and on the basis of reasonable belief, has refused or stated an intention of refusing to do anything that is a contravention of a provision of Division 1 or 1.1;
(c) the employee, acting in good faith and on the basis of reasonable belief, has done or stated an intention of doing anything that is required to be done in order that a provision of Division 1 or 1.1 not be contravened; or
(d) the employer believes that the employee will do anything referred to in paragraph (a), (b) or (c).

Saving

(2) Nothing in this section impairs any right of an employee either at law or under an employment contract or collective agreement.

These protections have been maintained in Bill C-11, the bill that was just introduced into the House of Commons that would thoroughly overhaul *PIPEDA*.

> **Recommendation 4.4: Provide whistleblower protection to employees of public bodies to protect them from reprisals for taking actions to prevent contravention of the *Act*.**

Definition of "use of personal information"

Although the word "use" is to be found throughout *ATIPPA, 2015*, it is not a defined term. *PHIA* defines "use" as "to handle or deal with the information or to apply the information for a purpose and includes reproducing the information, but does not include disclosing the information."

> **Recommendation 4.5: Provide a definition of "use of personal information" consistent with that found in *PHIA*.**

Prospective Complaints

Section 73 provides for the right to make a complaint about the collection, use or disclosure of personal information in contravention of *ATIPPA, 2015*. The right applies to an individual complainant about the collection, use or disclosure of their own information (section 73(1)), an individual complainant on behalf of another person with consent (section 73(2)), or the Commissioner to initiate an own motion investigation. In all instances, the collection, use or disclosure is referred to in the past tense, ie, where the allegation is that there has *already been* a collection, use or disclosure in contravention of *ATIPPA, 2015*.

In public sector privacy legislation across Canada, the right to complain is usually retrospective, as it is in *ATIPPA, 2015,* or vague. There is no explicitly prospective right.

PHIA, meanwhile, provides for a complaint against a prospective contravention of the *Act*, at section 66:

> *66(3) Where an individual believes on reasonable grounds that a custodian has contravened or is about to contravene a provision of this Act or the regulations in respect of his or her personal health information or the personal health information of another, he or she may file a complaint with the commissioner.*

This prospective right exists in other health privacy legislation, such as Ontario's *Personal Health Information Protection Act*, at section 56:

> *56(1) A person who has reasonable grounds to believe that another person has contravened or is about to contravene a provision of this Act or its regulations may make a complaint to the Commissioner.*

There are many circumstances whereby it would be appropriate to allow a privacy complaint to be of a prospective nature. For example, if an individual becomes aware of a new program involving a collection, use or disclosure of their personal information, and they have a reasonable basis to believe that it is contrary to *ATIPPA, 2015*, they should be able to file a complaint before the collection, use or disclosure is under way. From our perspective overseeing compliance with *ATIPPA, 2015*, one of the most important

roles we can play is to *prevent* privacy breaches *before* they can occur. Other provisions, such as the privacy impact assessment provision in section 72(3) and (4) and the requirement to consult with the OIPC on draft bills in section 112 reflect the same intent.

In some cases, we have become aware of programs or activities or public bodies through the media or through calls from people who do not wish to take on the role of complainant, but who have concerns.[4] Often we are able to initiate engagement with the public body on such issues and ensure that privacy concerns are addressed. Initiating that dialogue is typically our first course of action. Sometimes this is before implementation, other times after. Clearly, there are many reasons why it is much better to be able to initiate that dialogue before a program is implemented.

As noted, when we have heard through informal channels about privacy concerns regarding a program or policy before it is implemented, our preferred option is to open a dialogue with the public body to learn more about it, and then to suggest ways to address those concerns. We have had significant success with this approach, however public bodies do not always agree with us. If serious privacy concerns exist with a program or policy that has not yet been initiated, we believe it is important for us to be able to proceed with a formal investigation before personal information has been collected, used or disclosed, potentially in conflict with *ATIPPA, 2015*. This would require an amendment to section 73(1), (2) and (3) to make it clear that a privacy complaint can be either prospective or retrospective in nature.

This could be accomplished through the addition of language in each subsection as follows in **bold**:

> *73(1) Where an individual believes on reasonable grounds that his or her personal information has been**, or is about to be**, collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the commissioner.*
>
> *(2) Where a person believes on reasonable grounds that personal information has been**, or is about to be,** collected, used or disclosed by a public body in contravention of this Act, he or she may file a privacy complaint with the commissioner on behalf of an individual or group of individuals, where that individual or those individuals have given consent to the filing of the privacy complaint.*
>
> *(3) Where the commissioner believes that personal information has been**, or is about to be,** collected, used or disclosed by a public body in contravention of this Act, the commissioner may on his or her own motion carry out an investigation.*

Recommendation 4.6: Amend *ATIPPA, 2015* to allow prospective privacy complaints.

Enhanced Requirements for Privacy Impact Assessments

The Privacy Impact Assessment (PIA) is a well-recognized self-assessment tool that public bodies can use to help determine whether current or planned programs or policies are compliant with the privacy provisions of *ATIPPA, 2015*. While such assessments must be conducted under specific circumstances by

[4] https://www.cbc.ca/news/canada/newfoundland-labrador/nlc-changes-delivery-rules-1.5571017

departments and branches of the executive government under section 72 of *ATIPPA, 2015*, it is not a legal requirement for most public bodies.

Definition

The term "privacy impact assessment" first appears in the definition section of *ATIPPA, 2015*. Section 2(w) states:

> *"privacy impact assessment" means an assessment that is conducted by a public body as defined under subparagraph (x)(i) to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act;*

Section 2(x) defines public body, with 2(x)(i) referring to a specific category of public bodies: "a department created under the Executive Council Act, or a branch of the executive government of the province."

A PIA is an extremely useful tool in ensuring and documenting compliance with the requirements of the *Act*, and it is one that we often recommend as a best practice. At times, a PIA can be one of the steps that are "reasonable in the circumstances" to protect personal information in accordance with section 64. It is therefore important that the definition of Privacy Impact Assessment stand on its own in a separate provision, rather than being tied directly to a specific group of public bodies which may be required to conduct them under certain circumstances. It is our view that even if a PIA is not required under section 72, conducting one for certain types of projects might be consistent with the requirements of section 64, or simply a best practice that we would encourage. An appropriate model for this would be the one recently introduced with the passage of Northwest Territories Bill 29, An Act to Amend the Access to Information and Protection of Privacy Act[5]:

> *25.1. The following is added after section 42:*
>
> *Definition: "privacy impact assessment" 42.1. (1) In this section, "privacy impact assessment" means an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or service, including a common or integrated program or service, meets or will meet the requirements of this Part.*

> **Recommendation 5.1: Amend the definition of "privacy impact assessment" in such a way to make it similar to the one in the Bill amending the NWT ATIPPA and remove the reference to a specific class of public bodies from the definition in section 2(w).**

Expanded Applicability of PIA Requirements

As mentioned above, section 72 of *ATIPPA, 2015* addresses PIAs and preliminary PIAs, establishing the category of public bodies to which the requirement applies, as well as when a PIA must be shared with OIPC:

[5] Although passed by the legislature in 2019, those amendments to the *Access to Information and Protection of Privacy Act* have not yet been proclaimed into force.

72. (1) A minister shall, during the development of a program or service by a department or branch of the executive government of the province, submit to the minister responsible for this Act

(a) a privacy impact assessment for that minister's review and comment; or

(b) the results of a preliminary assessment showing that a privacy impact assessment of the program or service is not required.

(2) A minister shall conduct a preliminary assessment and, where required, a privacy impact assessment in accordance with the directions of the minister responsible for this Act.

(3) A minister shall notify the commissioner of a common or integrated program or service at an early stage of developing the program or service.

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

Section 72 in its current form misses many significant public body initiatives involving the collection, use and disclosure of personal information because of its limited application to departments and branches of executive government. This is partly due to the current definition which limits privacy impact assessments to a department or branch of executive government, combined with the language in section 72 that refers exclusively to the role played by "a" minister or "the" minister. This excludes major public bodies such as the Royal Newfoundland Constabulary; educational bodies, such as the Newfoundland and Labrador English School District; health care bodies, such as the Regional Health Authorities; and major municipalities, such as the City of St. John's. Many of these public bodies handle large volumes of personal information, some of which would likely be considered sensitive.

Section 72 should therefore be expanded to include all public bodies, with the exception of public bodies that are municipalities subject to the *Municipalities Act*. Options for how this can be done will be discussed further below. The large municipalities in the province, including Mount Pearl, St. John's, and Corner Brook, have their own individual statutes. In Newfoundland and Labrador, sizes of municipalities vary greatly, from the smallest (Tilt Cove with a population of 5 in 2016) to our three incorporated cities. It is reasonable to expect the larger municipalities to have the ability and resources to conduct robust privacy assessments when required. Further, the larger municipalities tend to deliver a greater variety of programs and services, and hold larger amounts of personal information of residents. On the other hand, the smaller municipalities handle smaller volumes of personal information and some do not have the capacity or expertise to complete a PIA. Some small municipalities do not even have full-time staff.

As all public bodies are already expected to be in compliance with the privacy provisions of *ATIPPA, 2015*, such an expansion should not create significant additional hardship, and the exclusion of municipalities subject to the *Municipalities Act* should not create too large a gap. A requirement for public bodies to conduct privacy assessments in order to identify and mitigate privacy risks in their programs or activities would likely improve compliance with *ATIPPA, 2015* and thereby protect the privacy of citizens. Doing so also has the benefit of documenting those assessments, which ensures that they are able to demonstrate good faith compliance efforts in case of a privacy complaint or breach.

For the benefit of public bodies that are required to complete a PIA for a common or integrated program or service, or for any public body undertaking a significant new program or service that involves the collection, use or disclosure of personal information, this Office has completed two documents to support them: a PIA expectations piece and another detailing our PIA Review Criteria. We are also available to support public bodies with feedback at any point along the way as they conduct privacy assessments.

> **Recommendation 5.2: Amend 72(3) and 72(4) to broaden its scope, such that any public body other than a local government body defined in 2(o)(iv) is required to notify the Commissioner of a common or integrated program or service at an early stage, complete a privacy impact assessment for such an initiative, and to submit the privacy impact assessment to the Commissioner for review.**

Definition of Common and Integrated Program

While some public bodies share courtesy copies of PIAs with the OIPC to seek informal feedback, the only mandatory submission of a PIA to the OIPC is when a minister identifies a program or service as being common or integrated. The concept of common or integrated programs or services first appeared in *ATIPPA* with the Bill 29 amendments. That amendment to the disclosure of personal information provision (then section 38(1)(u), now 68(1)(u)) is as follows:

> *68(1) A public body may disclose personal information only…*
>
> > *(u) to an officer or employee of a public body or to a minister, where the information is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or minister to whom the information is disclosed.*

Note that 68(1)(u) authorizes disclosure of personal information by any public body. Unlike section 72, it is not limited to departments of executive government. We therefore have a circumstance where a disclosure is permitted in 68(1)(u), however the protection factor in the form of a section 72 PIA only applies to departments or branches of executive government.

When the Bill 29 amendments added this lone provision for disclosure for common or integrated programs or services, it joined Prince Edward Island's Freedom of Information and Protection of Privacy Act, Manitoba's Freedom of Information and Protection of Privacy Act, and Alberta's Freedom of Information and Protection of Privacy Act; all three contain a lone reference to common or integrated programs or services in their disclosure sections.[6]

---

[6] Prince Edward Island's *Freedom of Information and Protection of Privacy Act*:
37 (1) A public body may disclose personal information only
(g.1) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed;

Manitoba's *Freedom of Information and Protection of Privacy Act*:
44(1) A public body may disclose personal information only

That Bill 29 amendment increased data-sharing possibilities in section 39, meaning that new programs could be created and information disclosed that was collected for another program and for another purpose, without an assessment as to the impact this would have on personal privacy.

The OIPC, in its initial submission to the 2014 *ATIPPA* Statutory Review Committee, pointed out this change, and requested that a PIA be required for such disclosures and that the Commissioner's Office review the PIA**.** The summary recommendations in the OIPC's initial submission read:

> *3. The ATIPPA should be amended to ensure that all PIAs that relate to a "common or integrated program or activity or a data-linking initiative" or any disclosure under section 39(1)(u) must be provided to the Commissioner for the Commissioner's review and comment. For reference, see section 69 of British Columbia's FIPPA.*

On page 85 of the full report, the Committee stated:

> *The Committee concluded that prevention is the optimal way of protecting personal information, and it can be achieved by clearly spelling out in the ATIPPA the following statutory obligations. The first requirement is for departments to carry out privacy impact assessments where personal information is involved in the development of new government programs and services and to submit them to the minister responsible for the ATIPPA for review and comment. Second, PIAs would also be forwarded to the Commissioner for his review and comment if they pertain to departments that address a common or integrated program or service for which disclosure of personal information may be permitted under section 39(1)(u).*

The Committee made the recommendation, starting on page 68 of the Executive Summary, that:

> *65. With respect to the role of the Commissioner in protection of personal information that the Act provide for: e. The Commissioner having the duty to review a privacy impact assessment developed by a department of government for any new common or integrated program or service for which disclosure of personal information may be permitted under section 39(1)(u).*

The result was section 72, which represents a step forward in privacy protections. However, the term "common or integrated" is not defined in the *Act*, which has led to differing interpretations. After extensive research, the OIPC adopted the definition contained in British Columbia's *Freedom of Information and Protection of Privacy Act*, while the ATIPP Office adopted a definition developed by Service Alberta in FOIP Bulletin #8. This represents an ongoing disagreement which could be resolved through greater clarity in the statute. To assist in this process, we conducted a jurisdictional scan of such

---

(f.1) to an officer or employee of a public body, for the purpose of delivering a common or integrated service, program or activity, if the information is necessary to deliver the service, program or activity and the officer or employee to whom the information is disclosed needs the information to carry out his or her responsibilities;

Alberta's *Freedom of Information and Protection of Privacy Act*:
40(1) A public body may disclose personal information only
(i) to an officer or employee of a public body or to a member of the Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and for the performance of the duties of the officer or employee or member to whom the information is disclosed,

definitions contained in legislation or regulations. The definitions from the legislation in BC, NB, SK and NT is available at Appendix D.

> **<u>Recommendation 5.3</u>: Amend section 2 to add a definition of the term "common or integrated program or service."**

Since *ATIPPA, 2015* came into force in June 2015, the OIPC has received two notifications of common or integrated programs or services – the Digital by Design Initiative (MyGovNL platform) and the eProcurement system. The Department of Finance also consulted with OIPC on what they deemed to be a potential common or integrated initiative - the consolidations of collections.

We suspect that some initiatives are not being recognized as common or integrated because of the lack of a clear statutory definition. Further, as noted above, with the definition of Privacy Impact Assessment in section 2(w) being confined to a specific group of public bodies, some common or integrated initiatives that could benefit from a robust PIA that would be reviewed by the OIPC may not be going through such a process. For example, the provincial government has initiated a shared health model under which certain public bodies within the health sector are leading initiatives on behalf of the others. A common procurement service is being led by Central Health on behalf of all four Regional Health Authorities (RHAs) and the Newfoundland and Labrador Centre for Health Information (NLCHI). NLCHI, in turn, is leading the eHealth strategy and, as part of that initiative, is developing such things as a Workforce Management System. To be clear, we have been consulted on both of these initiatives and this is a testament to the good relationship that the OIPC has with these entities. The point here is that, as they are not departments of the executive branch of the provincial government, there is no statutory obligation for them to do a PIA or consult this Office on it. With more innovative approaches to public services being explored involving greater collaboration between public bodies, we anticipate that there will be more such examples.

Information Sharing Agreements and Common or Integrated Programs or Services

Another useful tool required in some jurisdictions for a common or integrated program or service is an Information Sharing Agreement. This is a particularly useful piece when one or more of the parties to the initiative are not public bodies subject to *ATIPPA, 2015*. Further, these written agreements, if done well, contain many of the same details one would expect to find in a PIA. As such, much of the work would already be documented.

Key components of any such agreement include a description of the initiative, including the purpose and expected outcome of the initiative; identification of the personal information involved; provisions regarding expected safeguards and future use and/or disclosure of information obtained as part of the initiative; description of the roles and responsibilities for participating entities; provisions surrounding any withdrawal from the initiative or termination; the effective dates for the information sharing; and any other information deemed appropriate for the initiative. The final agreement should be signed by individuals in positions of authority, typically the head of the public bodies participating in the initiative.

Appendix E contains three examples of legislative language, from BC, SK and NB, that could be used as a model.

Recommendation 5.4: Amend section 72 to add a requirement for an information sharing agreement to be completed by parties to a common or integrated program or service.

Biometrics

It has always been recognized within the privacy field that some personal information is more sensitive than other personal information, and the sensitivity of the information must influence how it is treated. This is reflected in section 64, which requires public bodies to take steps that are "reasonable in the circumstances" to protect personal information.

Some of the most sensitive personal information that exists is biometric information. One of the basic reasons for this is its immutability. In the case of a privacy breach that could cause harm, such as identity theft, a new identification card or identifying number can be issued. In the case of a theft of information derived from a person's fingerprint or face, there is no possibility of replacing the information, and therefore mitigating, the effect of the breach. Vendors of biometric systems assert that because the biometric characteristics are broken down into digital information using a proprietary algorithm, that even if the information is breached, it cannot be used to reconstruct an identity. While this no doubt helps to assure potential purchasers about the security of such systems, it is not necessarily borne out by the research, which suggests that inverse biometrics may be feasible, allowing the original biometric identifier to be reconstructed.

For these reasons, biometric information is deserving of the strongest statutory protection we can give it. Furthermore, not only should it be protected once it is collected, but there should be a high necessity threshold for the collection of biometric information. In the examples we have seen to date where biometric information has been or is intended to be collected, we question whether such a threshold has in fact been met. On the contrary, because of the proliferation of cheaper and cheaper technology for facial recognition, fingerprint scanners and more, the temptation will be there for public bodies to adopt biometric technologies for convenience and efficiency rather than necessity. If saving a dollar in service delivery becomes the established necessity threshold, privacy becomes meaningless.

The federal Office of the Privacy Commissioner (OPC) in 2011 created guidance on the use of biometrics entitled Data at Your Fingertips: Biometrics and the Challenges to Privacy. The OPC has indicated that it is currently in the process of updating its guidance on the use of biometrics, and has been consulting with Commissioners across Canada for that purpose. The most recent publication by privacy oversight bodies in Canada regarding biometrics was released on October 29, 2020, which was a joint Investigation Report on the use of facial recognition by Cadillac Fairview Corporation, conducted by the Alberta, British Columbia and Federal Commissioners.

It is now past time for *ATIPPA, 2015* to ensure that biometric information is explicitly referenced and defined in the statute; that an explicitly high standard be put in place to ensure that biometric technology is not used more than is necessary in the collection, use and disclosure of personal information by public bodies; and that appropriate oversight exists to ensure that the legislative standards are adhered to.

In terms of a definition, at present *ATIPPA, 2015* contains the following:

> *2(u) "personal information" means recorded information about an identifiable individual, including*
>
> *[…]*
>
> *(v) the individual's fingerprints, blood type or inheritable characteristics,*

While fingerprints are biometric in nature, there are a number of other types of biometric information including facial recognition, and less well known ones such as gait recognition.

Biometrics or biometric information refer to measurable characteristics used to identify an individual. The information can be used to digitally identify a person or allow them to access systems, devices or data. Biometric information or "identifiers" are often genetic or inheritable characteristics and include fingerprints, facial patterns, vocal recordings, and DNA, for example.

Facial recognition is of particular concern because of the potential for collection of the information without the knowledge, let alone consent, of the individual. Facial recognition capability can be baked into the software for stationary video surveillance systems or mobile body cameras. Facial recognition software has been used to crawl the internet, identifying people from pictures that are available in the public domain on the internet and even scraping data from social media profiles. The power of this technology to create comprehensive databases of personal information without knowledge or consent makes facial recognition technology one of the most alarming technological trends for privacy experts around the world. The prospect of the mass collection of biometric information beyond facial recognition, such as heat signatures and weight sensors, in a combined public/private context are not as futuristic as they may sound, as both of these elements were part of the now-defunct Google Sidewalk smart city proposal in Toronto.

Although the use of the term "including" in section 2(u) means that the definition is not limited to the characteristics listed, the significance of biometric information in terms of its sensitivity means that it should be explicitly listed. Furthermore, because we propose that additional statutory provisions be created regarding biometric information, it would also be appropriate to include a definition of that term.

Two provincial public sector privacy laws include the term "biometric" (underlining added):

Prince Edward Island's *Freedom of Information and Protection of Privacy Act*:

> *1 (i) "personal information" means recorded information about an identifiable individual, including…*
>
> *(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,*
>
> *1 (a.2) "biometric information" means information derived from an individual's unique measurable characteristics;*

and Alberta's *Freedom of Information and Protection of Privacy Act*:

1 In this Act, (b.1) "biometric information" means information derived from an individual's unique measurable characteristics;

> *1 (n) "personal information" means recorded information about an identifiable individual, including …*
>
> *(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,*

Internationally, the European Union's General Data Protection Regulation (GDPR) provides an example when it comes to biometrics. The GDPR identifies some types of data as more sensitive and provides extra protection. These include, but are not limited to, genetic data and biometric data. The GDPR defines biometric data in Article 4(14):

> *'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.*

Simply defining biometric information and including it in the definition of personal information will not provide the additional protection it needs, to reflect its degree of sensitivity and immutability. Few statues in Canada have yet done this, however Quebec's *Act to Establish a Legal Framework for Information Technology* does to some extent. This Act specifically references biometrics and applies best practices, such as minimizing collection and independent oversight:

> *Division II – Modes of Identification and Location*
>
> *44. A person's identity may not be verified or confirmed by means of a process that allows biometric characteristics or measurements to be recorded, except with the express consent of the person concerned. Where consent is obtained, only the minimum number of characteristics or measurements needed to link the person to an act and only such characteristics or measurements as may not be recorded without the person's knowledge may be recorded for identification purposes. No other information revealed by the characteristics or measurements recorded may be used as a basis for a decision concerning the person or for any other purpose whatsoever. Such information may only be disclosed to the person concerned, at the person's request. The record of the characteristics or measurements and any notation relating thereto must be destroyed as soon as the purpose of verification or confirmation of identity has been met or the reason for the verification or confirmation no longer exists.*
>
> *45. The creation of a database of biometric characteristics and measurements must be disclosed beforehand to the Commission d'accès à l'information. As well, the existence of such a database, whether or not it is in service, must be disclosed to the Commission. The Commission may make orders determining how such databases are to be set up, used, consulted, released and retained, and how measurements or characteristics recorded for personal identification purposes are to be archived or destroyed. The Commission may also suspend or prohibit the bringing into service or order the destruction of such a database, if the database is not in compliance with the orders of the Commission or otherwise constitutes an invasion of privacy*

Although this Quebec law is a singular example in Canada, it must also be reflected that it is nearly 20 years old, and the technology facilitating the collection, use and disclosure of biometric information, not to mention the proliferation of big data, artificial intelligence, and the internet, mean that the potential collections, uses and disclosures as well as privacy risks have increased exponentially since it was introduced. That being said, our colleagues in Quebec have recently issued an excellent plain language guidance piece on biometrics that reflects the legislation in that jurisdiction, which demonstrates that it is substantially ahead of this and other Canadian jurisdictions in its approach to biometrics.

We therefore recommend the following in relation to biometric information:

> **Recommendation 6.1: That section 2(u)(v) be amended to state: "(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics";**
>
> **Recommendation 6.2: That biometric information be defined as it is found in the Alberta and PEI statutes: "Biometric information" means information derived from an individual's unique measurable characteristics.**
>
> **Recommendation 6.3: That a privacy impact assessment be required for any program or initiative involving the collection, use or disclosure of biometric information, including changes or expansions to existing programs. Furthermore, the OIPC should be notified of the development of any program involving the creation of a biometric database prior to its creation or use, and the privacy impact assessment should be provided to the OIPC for review and comment prior to system implementation. Such an amendment could potentially be located in a new section 72(5).**

Artificial Intelligence

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

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

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

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

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

If we were to adopt an approach purely from a privacy perspective, AI would be a non-starter based on data minimization alone. We do, however, recognize that AI promises not only risks, but great benefits to society. On that basis, privacy and AI experts the world over are attempting to develop a framework that works for both.

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

- Decisions made by federal government departments are data-driven, responsible, and comply with procedural fairness and due process requirements.
- Impacts of algorithms on administrative decisions are assessed and negative outcomes are reduced, when encountered.
- Data and information on the use of Automated Decision Systems in federal institutions are made available to the public, where appropriate.

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

Realistically, in Newfoundland and Labrador, we are unlikely to see the creation of a separate Data Commissioner in the foreseeable future. We are, however, likely to see AI and automated decision-making

at some point, and perhaps sooner rather than later, in light of the rate of expansion of this technology around the world. In a small jurisdiction, one often needs to wear several hats. While AI creates substantial challenges for effective oversight of legal and ethical implications, there is already a substantial overlap with privacy oversight that positions the OIPC well to take on that role. Some of the challenges inherent in attempting to apply a traditional privacy lens to AI, without alteration or augmentation, was captured recently by Ontario's Information and Privacy Commissioner in her comments on the creation of a new privacy statute in that province:

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

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

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

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

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

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

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

Recommendation 7.4: In addition to privacy and access to information issues, in its review and assessment, the OIPC should be entitled to comment on all implications for the use of AI in the proposed program, including data ethics factors such as proportionality, fairness and equity, in a manner comparable to a Data Commissioner; to this end, amendments to the purpose of the *ATIPPA, 2015* would be required to reflect the added mandate for an independent oversight agency that is empowered to review and comment on the implications, including privacy and data ethics implications, for the implementation of artificial intelligence in public body programs. Comparable powers or duties would need to be added to section 95.

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

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

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

Political Parties

In Canada, no public sector access and privacy legislation applies to the collection, use or disclosure of personal information by political parties. Currently, only British Columbia's private sector *Protection of Personal Information Act* captures political parties within its scope. BC's Information and Privacy Commissioner published a substantial report on issues relating to privacy and political parties in 2019, entitled Full Disclosure: Political Parties, Campaign Data, and Voter Consent.

In this age of social media and big data, whereby political parties engage in micro-targeting of potential voters based on their demographic characteristics, the groups they belong to, the products they purchase, and many other indicators, it is clear that personal information of Canadians, often in minute, granular detail, is now at the core of modern sophisticated campaigns at the provincial and federal level. When power is at stake, as it is in the political process, such data is prone to misuse.

The right to privacy is a fundamental human right, and the collection of personal information by political parties should be subject to privacy protection. It might be possible to provide for this protection in a separate, stand-alone statute. However, it is our view that it could also be accomplished by amendments to *ATIPPA, 2015*. There are several such amendments that, together, would accomplish this goal.

Canada's Federal, Provincial and Territorial Privacy Commissioners issued a joint resolution in 2018 calling on governments to create laws containing meaningful privacy obligations for political parties:

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

As noted in Privacy and the Electorate: Big Data and the Personalization of Politics,

> *Federal privacy legislation applicable to the private and public sectors does not currently cover the activities of political parties. The Personal Information Protection and Electronic Documents Act (PIPEDA), applicable to the private sector, does not appear to cover political activities because they are likely excluded from the definition of "commercial activities" in the legislation. Political parties are excluded from the definition of "government institutions" in the Privacy Act, the public-sector privacy legislation. The Canada Elections Act (CEA) does not significantly oversee the practices of political parties with regard to the collection, use, storage, and analysis of data about voters and donors. Numerous private sector entities are involved by collecting, analyzing, and selling voter data to political parties. It is unclear how the legislative framework applies to them or what privacy rules they apply to their own activities."*[7]

[7] Elizabeth Judge and Michael Pal, 2017, University of Ottawa Centre for Law, Technology and Society

Academics, privacy oversight bodies, and Canada's Chief Electoral Officer have all expressed the need for legislation to address the gap which allows political parties to operate without privacy laws or oversight. Alternatives to address this would appear to involve either substantial amendment to *ATIPPA, 2015* or a standalone statute. Although a standalone statute might be the better option in some respects, the perfect is often the enemy of the good. The value of bringing it forward in this context is that the *ATIPPA, 2015* is a statute that is currently under review, making it the most practical option available. Furthermore, it could be accomplished in an incremental way through inclusion in the *ATIPPA, 2015*. For example, if "registered political party" were to be added to the definition of public body, a provision of section 5 could be drafted to make it clear that the *Act* only applies to *personal* information collected, used, and disclosed by political parties, and the access to information aspect would therefore be limited such that individuals would only be able to access their own personal information. As for the privacy provisions, a number of those would also not be applicable, which could be referenced in section 5.

The process for an access to information request should apply to political parties as it currently exists, as well as appeal and oversight by the Commissioner. In terms of the privacy provisions, again, some would not be applicable to political parties; however even if section 64 were to apply, along with the privacy complaint and oversight provisions, this would be a significant step forward. By proceeding in this incremental fashion, the efficacy of this approach could be reconsidered and potentially expanded at the next statutory review of *ATIPPA, 2015*.

> **Recommendation 8.1: broaden the scope of *ATIPPA, 2015* to include political parties by adding "registered political party" to the definition of a public body in section 2; and make corresponding amendments to section 5 to limit the access to personal information collected, access and used by political parties; and make further amendments to section 5 to ensure that only the appropriate privacy sections of the Act apply to political parties.**

The Public Interest

The ways in which heads of public bodies are mandated to consider the public interest has been a topic of a number of discussions and reports over the years.

Section 9 provides two caveats to the exceptions to access in *ATIPPA, 2015*. Broadly, they are:

- The non-application of enumerated discretionary exceptions where it is clearly established that the public interest in the disclosure of the information outweighs the purpose for the exception, and
- A requirement for proactive disclosure, regardless of whether any exception would apply, of information about a risk of significant harm to the environment or to the health or safety of the public or a group of people, the disclosure of which is clearly in the public interest.

Section 9(1): The Public Interest Override

The public interest override at section 9(1) applies to several of the discretionary exceptions to access. In some instances, exceptions which are not included under section 9 include their own considerations of the public interest.

Exception	Type	Application of s. 9
27 – Cabinet confidences	Mandatory	Does not apply, but s. 27(3) provides for disclosure if Clerk satisfied that it is in the public interest
28 – Local public body confidences	Discretionary	s. 9 applies
29 – Policy advice or recommendations	Discretionary	s. 9 applies
30 – Legal advice	Discretionary	s. 9 applies
31 – Disclosure harmful to law enforcement	Discretionary	Does not apply
32 – Confidential evaluations	Discretionary	s. 9 applies
33 – Information from a workplace investigation	Mandatory	Does not apply
34 – Disclosure harmful to intergovernmental relations or negotiations	Discretionary	s. 9 applies
35 – Disclosure harmful to the financial or economic interests of a public body	Discretionary	s. 9 apples
36 – Disclosure harmful to conservation	Discretionary	s. 9 applies
37 – Disclosure harmful to individual or public safety	Discretionary	Does not apply
38 – Disclosure harmful to labour relations of public body as employer	Discretionary	s. 9 applies
39 – Disclosure harmful to business interests of a third party	Mandatory	Does not apply
40 – Disclosure harmful to personal privacy	Mandatory	Does not apply, but s. 40(5) does include consideration of public interest
41 – Disclosure of House of Assembly service and statutory office records	Mandatory	Does not apply

The public body bears the burden of proof in establishing the application of all exceptions other than when section 39 is asserted by a third party. A public body is required to disclose information to which one of the enumerated exceptions apply if the public interest in disclosure is "clearly demonstrated" to outweigh the reasons for the exception; however, the burden of proof for such a demonstration is not

explicit. Section 9 does not reverse the burden of proof in section 43, and from a practical standpoint, if the applicant does not have the records, they may not be in the best position to argue that disclosure is in the public interest, except perhaps from a high level perspective based on the subject matter of the request. Lacking specificity on the burden of proof in section 9, courts have interpreted the statute as they find it.

In *Mastropietro v. Newfoundland and Labrador (Education)*, Justice Murphy commented that:

> *[49] In my view it would also be open to the party bearing the onus to present evidence on an appeal on the issue of the public interest in disclosure. As noted earlier, an appeal to this Court is a new matter or a hearing de novo and section 59(1) of the Act specifically provides that the Court may receive evidence by affidavit. I note that the foregoing provision is permissive in nature and does not preclude the Court from receiving evidence in other forms.*
>
> *[50] I am not saying that it is incumbent upon a person seeking to establish that there is a sufficient public interest in disclosure so as to outweigh the purpose of the exception from disclosure, to present evidence of the public interest in disclosure, in every case. There may well be cases where the public interest in disclosure, is so notorious as to be capable of judicial notice by the Court. There may be other cases, where the records or documents themselves, are such that the Court is able to conclude there is a public interest in disclosure. However, in the absence of these or other similar circumstances, it is my view, that a person seeking to argue on an appeal, that the public interest in disclosure clearly outweighs the purpose of the exception from non-disclosure would be well advised to present evidence to the Court to support such an argument.*

Changes that could clarify the burden of proof warrant consideration in this review.

> **<u>Recommendation 9.1</u>: Clarify that the burden of proof in the application of the public interest override does not rest solely on the applicant or the public body but that any party, including the OIPC at the review stage, is obligated to bring forward evidence that could be relevant to this determination.**

A possible omission in section 9 is its non-application to section 39 (business interests of a third party). This is a mandatory exception like section 40, but unlike section 40 (personal privacy), it does not contain any provisions that could allow for disclosure in the public interest, such as those in 40(5). It is perfectly conceivable that information which may be injurious to the narrow business interests of a third party may nonetheless be of great public interest, and that public interest could outweigh the rationale of protecting a third party business against the harm from the disclosure of its business information.

The federal *Access to Information Act* provides for consideration of the public interest with respect to third party business information. Section 20 directs a public body to withhold third party information that meets a similar three-part test as found in *ATIPPA, 2015*. However, section 20(6) provides:

> *Disclosure authorized if in public interest*
>
> *(6) The head of a government institution may disclose all or part of a record requested under this Part that contains information described in any of paragraphs (1)(b) to (d) if*

(a) the disclosure would be in the public interest as it relates to public health, public safety or protection of the environment; and

(b) the public interest in disclosure clearly outweighs in importance any financial loss or gain to a third party, any prejudice to the security of its structures, networks or systems, any prejudice to its competitive position or any interference with its contractual or other negotiations.

In terms of the kind of public interest over-ride found in section 9(1), although it is found in some international jurisdictions, the model in *ATIPPA, 2015* is not the most common in Canada:

Canada	No general public interest override	Public interest override for third party
British Columbia	No general public interest override	
Alberta	No general public interest override	
Saskatchewan	No general public interest override	Public interest override for third party
Manitoba	No general public interest override	Public interest override for third party
Ontario	General public interest override	
Quebec	General public interest override	
New Brunswick	No general public interest override	Public interest override for third party
Nova Scotia	No general public interest override	
P.E.I.	No general public interest override	
Yukon	No general public interest override	
N.W.T.	No general public interest override	
Nunavut	No general public interest override	

Recommendation 9.2: Include third party business information (section 39) among the list of exceptions to access to which the public interest override in section 9(1) applies.

Section 9(3): Mandatory Proactive Disclosure

The second part of section 9 is even broader and operates regardless of any of the exceptions in *ATIPPA, 2015* and even in the absence of an access to information request:

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

We considered the proactive disclosure requirements of section 9 in A-2020-005 and also commented on it in P-2020-002, 2007-006 and 2007-003.

Similar provisions exist in other jurisdictions, such as Ontario:

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

And British Columbia:

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

Language similar to that in section 9(3) of *ATIPPA, 2015* is also found in New Brunswick, Prince Edward Island and Alberta.

However, British Columbia's interpretation of section 25 gives us some concern in that the use of "without delay" has been taken to require a sense of urgency or immediacy. Without an immediate problem, section 25 has been found not to apply. See, for example, Order 02-38:

> *[53] As the applicant notes, in Order 01-20 and other decisions, I have indicated that the disclosure duty under s. 25(1)(b) is triggered where there is an urgent and compelling need for public disclosure. The s. 25(1) requirement for disclosure "without delay", whether or not there has been an access request, introduces an element of temporal urgency. This element must be understood in conjunction with the threshold circumstances in ss. 25(1)(a) and (b), with the result that, in my view, those circumstances are intended to be of a clear gravity and present significance which compels the need for disclosure without delay.*

Quebec's override is found at section 41.1 of the *Act respecting Access to documents held by public bodies and the Protection of personal information*. Similar to section 9(1), it provides that certain exceptions to access do not apply in the case of "immediate hazard to the life, health or safety of a person or a serious or irreparable violation of the right to environmental quality, unless its disclosure would likely seriously interfere with measures taken to deal with such a hazard or violation." This limitation to "immediate hazard" would align it with the British Columbia OIPC's interpretation, although BC's statute lacks explicit reference to an immediate hazard as the trigger.

The potential to interpret section 9(3) of *ATIPPA, 2015* to include a required element of temporality is unnecessary. One could imagine a threat to health, safety or environmental harm that was gradually emerging and it was in the public interest to have this information disclosed before the matter became urgent. The need to have evidence that clearly demonstrates the risk of harm necessarily implies that urgency is one of the considerations, but we recommend that the section be clarified to avoid automatically excluding cases that do not have immediacy of risk as a fundamental feature.

Recommendation 9.3: Consider amending section 9(3) to remove the potential for limitation of its applicability to matters that are "urgent" as a temporal consideration.

Third Party Business Interests

The Report of the 2014 Statutory Review of the *ATIPPA* contains a chapter at section 3.6 on this topic. It found that public bodies had pushed the previous Cummings Review to weaken the right of access when it comes to information relating to third party business dealings with public bodies. The 2014 Committee's recommendation led to section 39 of *ATIPPA, 2015*, which restored the three-part harms test that is the most common Canadian model for a third party business interests exception. As noted in our submission to the 2014 Review, jurisdictions operating with the three-part harms model that is now in *ATIPPA, 2015* have been doing so for decades. Fears that third parties will no longer do business with public bodies unless access to information is weakened have not been borne out. Interestingly, in the 2014 Review it was representatives of the business community who argued for greater transparency with government.

In addition to restoring the three-part test in section 39 as it existed prior to Bill 29, the *ATIPPA, 2015* also saw a new notification regime in section 19. The Committee explained that other notification regimes tended to result in an unnecessary level of notification of third parties. In particular, the 2014 Statutory Review Committee amended the third party notification provision so that the first notification occurs under section 19(1) when the public body formed an *intention* to release information that might be excepted from disclosure, rejecting the model whereby public bodies must notify when they are *considering* whether to disclose information. An appeal opportunity is then provided under 19(5) when the public body has made a decision to disclose. If an appeal is filed, the disclosure does not occur until all appeals are exhausted. We agree with that approach.

One of the reasons we agree with the notification provision crafted by the 2014 ATIPPA Review Committee is that a very high percentage of third party appeals are lost by third parties, and the information is ultimately disclosed anyway. In those circumstances, access to information is delayed substantially, particularly if the third party skips the OIPC process and goes directly to court, or if they appeal to court following the OIPC process.

One of the advantages of the three part harms test as currently found in the *ATIPPA, 2015* is that it is shared with the larger jurisdictions of Alberta, British Columbia and Ontario. As a result, decades of jurisprudence has been developed, and there is a great deal of clarity regarding the interpretation of this exception. We also have the benefit of a Newfoundland and Labrador Court of Appeal decision (*Corporate Express*) which ruled on the third party business exception.

While the OIPC has issued numerous third party Commissioner's Reports, the vast majority have found that the exception does not apply and the information should be released. A relatively small number of these Reports have become the subject of court appeals. Even when court appeals have been filed, there has yet to be a case where the third party has, in the end, prevented the release of information that the public body had decided to release.

There may be a number of reasons for this. One is that public bodies are relatively cautious about deciding to release third party information. They may in fact be refusing access to information in clear-cut cases without the need to notify third parties, and perhaps these decisions are not being appealed. The other, more likely explanation, is that government typically does not collect the kind of information intended to be protected by section 39. One presenter, quoted in the 2014 Statutory Review Report, put it this way: "Well, I guess I can say do we have a right to know what the public body paid for a stapler. It is not the Colonel's secret that we're asking for. It is not for the components that go into manufacturing a widget..."

When government is procuring widgets, they are typically just buying them, not inquiring into the manufacturing process for widgets. If a public body is purchasing a chicken dinner, they are not typically requiring the Colonel to submit a copy of his recipe. While there are undoubtedly circumstances where public bodies do require proprietary information of third parties, section 39 is available to ensure that such information is not disclosed.

Why then, do third parties even file appeals, when public bodies are typically cautious about releasing third party information, and section 39 is only meant to cover a limited set of information? In our experience, some companies are not knowledgeable about government access to information laws. Receiving a notice under section 19 may be the first time they have even heard of it. Perhaps the majority of their customers are in the private sector, where this issue doesn't normally arise. The reaction from such third party complainants can range from indignation to surprise. Sometimes matters are resolved informally by explaining the statute and the three-part test, and that the third party bears the burden of proof to establish that section 39 applies. Other times these matters result in a Commissioner's Report, and rarely, a court appeal.

The ones that tend to proceed to court involve third parties that are, more often than not, national companies with legal departments. Filing a complaint with our Office costs nothing, whereas filing an appeal in court can be more costly. If a third party suspects the applicant might be an industry competitor, there is every incentive to file an appeal to delay access. While we cannot say with certainty that this has been the case in any individual appeal, a pattern has certainly emerged.

Third Party	Public Body	Date of Access Request	Report	Date of Report	Court Docket	Court Outcome	Date of Decision	Total Days
Coporate Express	Memorial University	28-Aug-12	A-2013-009	4-Jun-13	2013 01G 3476	Appeal Dismissed	30-Oct-15	1,158
Coporate Express	Memorial University	28-Aug-12	A-2013-009	4-Jun-13	2014 01H 0085 (CA)	TP Claim Dismissed	19-Sep-14	
Coporate Express	Memorial University	13-Jun-14	A-2014-013	12-Dec-14	2015 01G 0823 (TD)	Discontinued	14-Jun-16	732
Bell Canada	OCIO	17-Jun-15	A-2015-005	21-Oct-15	2015 01G 6086	Discontinued	28-May-17	711
Bell Canada	OCIO	29-Oct-15	A-2016-001	22-Feb-16	2016 01G 1709	Discontinued	20-Apr-18	904
Bell Canada	Eastern Health	6-Nov-15	A-2016-002	23-Feb-16	2016 01G 1761	Discontinued	31-Jan-18	817
Bell Canada	Health and Community Services	11-Aug-16	A-2016-030	19-Dec-16	2017 01G 0320	Discontinued	21-Feb-18	559
Bell Canada	Business, Tourism, Culture and Rural Development	30-Aug-16	A-2017-005	8-Feb-17	2017 01G 1296	Ongoing		1,546
Atlantic Lottery Corp.	Finance	13-Oct-16	A-2017-004	8-Feb-17	2017 01G 2004	Appeal Dismissed	19-Jun-18	614
Don Gibbons Limited	Health and Community Services	1-Nov-16	A-2017-009	10-Mar-17	2017 01G 2562	Discontinued	15-Dec-17	409
Bell Canada	Memorial University	24-Jan-17	A-2017-014	9-May-17	2017 01G 4033	Discontinued	26-Feb-18	398
McKesson Specialized Distribution Inc.	Health and Community Services	7-Sep-18	A-2019-001	7-Jan-19	2019 01G 0529	Discontinued	22-Nov-19	441
Bell Canada	OCIO	13-May-19	A-2019-026	26-Sep-19	2019 01G 6549	Ongoing		560
Bell Canada	City of Mount Pearl	9-Jan-20	A-2020-018	15-Sep-20	2020 01G	Ongoing		319

One of the things we have found is that no third party has yet won a claim in court, and in fact most appeals have been discontinued by the third party on the eve of a court hearing. It is our view that if the notification in section 19 were broadened that it would have no measurable impact on the protection of third party business information. In cases where notification is justified, third parties are receiving appropriate notification. However, if the bar is lowered, and public bodies were required to notify third

parties that today would not quite meet that threshold, based on the history of how this has played out, the chances of success of that additional class of third party claims would be very low indeed.

As addressed in several of our reports, public bodies have notified third parties when notification cannot be justified under section 19(1). In such cases, a public body will have received an ATIPP request where some or all of the responsive records pertain to a third party business. The public body has conducted an assessment, and concluded that section 39 does not apply. No doubt or uncertainty has been expressed in that assessment. However, on a number of such occasions, public bodies have proceeded to give a section 19 notice to third parties, despite the language in section 19 that notification is only triggered when the head intends to give access and the head also "has reason to believe" that the record or part of the record "contains information that might be excepted from disclosure."

Section 19 exists for circumstances that fall into a grey area, where there is a lack of certainty about whether or not section 39 applies. If the public body determines that section 39 applies, it is a mandatory exception and the public body must refuse disclosure. No notification is required, and the public body bears the burden of proof in the event of a complaint. If the public body determines that section 39 does not apply, it must disclose. Section 19 speaks to that "in-between" circumstance, where there is at least a "reason to believe" that section 39 "might" apply. Absent that reason, the information should be released to the applicant. What we have seen in some circumstances, however, is that the assessment has been completed by the public body, and a definitive conclusion has been reached that section 39 does not apply. However, whether out of an abundance of caution or a desire to maintain a positive relationship with a third party, the public body may issue a section 19 notification even when it is not warranted. This is not a neutral decision, as it can substantially impact the applicant's rights by significantly delaying disclosure where there are no grounds to do so.

In our view, the current notification regime already tips the balance very much in favour of ensuring that legitimate section 39 claims are protected, however we appreciate that this fulfils the purpose of the *Act* in section 3(2)(c)(iii). On the other hand, access to information applicants are sometimes required to wait years while an appeal is ongoing, only to see the matter withdrawn at the last minute or the appeal dismissed. We do not wish to see the scales tip further towards an over-notification or over-protection of third party information. If section 19 is to be amended at all, it should be amended to simply make it clear that section 19 notification should not occur unless the conditions described in 19(1) apply.

> **Recommendation 10.1: Consider whether an amendment may be necessary to indicate to public bodies that notification to third parties should not occur where the conditions described in 19(1) are not met. Otherwise, retain sections 19 and 39 as they currently exist.**

Indigenous Issues

Does *ATIPPA, 2015* sufficiently recognize and address privacy and access to information issues relating to Indigenous communities? We have not been presented with many specific issues that would raise this question, however there may be issues that have not come to our attention. We did, however, recently issue Report A-2020-020 regarding a request for access to information to the Intergovernmental and Indigenous Affairs Secretariat, which is now the subject of an application for a declaration under section

50. In light of the increasing awareness of concerns regarding Indigenous peoples in Canada, the time may be right during this legislative review to consider this question.

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

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

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

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

Commissioner Vacancy

Although there is a provision for the appointment of an Acting Commissioner in *ATIPPA, 2015*, and provision for the Commissioner to delegate their authority, there is no provision for the exercise of the Commissioner's authority in instances of their incapacitation or if the office is vacated in the absence of such delegation or appointment. There have been two month-long vacancies after the retirement or resignation of a Commissioner, and the failure to appoint an Acting Commissioner on a timely basis represents a serious reputational and legal risk to the OIPC which could also impact complainants, third parties or public bodies. It has been clearly demonstrated that the process for making such an appointment is not sufficient to meet the requirement of ensuring that there is a duly appointed Commissioner in place at all times.

Former Commissioner Ed Ring gave significant advance notice of his retirement, and he officially retired effective June 23, 2016. His replacement, Donovan Molloy, was not appointed until July 22, 2016. Former Commissioner Donovan Molloy resigned effective February 19, 2019, and an Acting Commissioner was not appointed until March 21, 2019.

The *ATIPPA, 2015* is written in such a way that every provision involving the exercise of the oversight role is one where the Commissioner is empowered to do something. In practice, many of these roles are delegated to staff in accordance with section 103. A compelling argument can be made that the oversight function can only legally operate where there is a Commissioner in place. A delegation by a Commissioner to staff arguably cannot survive when the Commissioner's role is vacant.

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

For example, section 44 outlines the investigative process. Each aspect of the process involves the Commissioner exercising authority under the statute, which is typically delegated to staff. Another highlight would be section 97, which has been contentious at times. We have seen public bodies refuse to cooperate with a demand for records by the Commissioner under this section. This, or another challenging circumstance, could easily occur during a period of Commissioner vacancy. While OIPC staff are knowledgeable in terms of carrying out the Office's oversight functions and are competent to take appropriate steps, without a Commissioner, no one can be said to have been delegated to take those steps.

Furthermore, we have a number of ongoing court matters at any given time that require direction to counsel. While OIPC senior staff are fully competent to direct counsel and carry on the work of the Office during these interim periods between Commissioner appointments, there is a very real concern that we have simply been fortunate that no public body, third party, applicant, or even news media have challenged our authority to do so. Despite some awkward questions that have been put to us during these periods of time, staff have carried on with investigations, accepted new complaints, and operated as if in a caretaker mode. Whether through luck or good faith on the part of the parties we deal with, staff have not yet been formally challenged on their authority to conduct oversight business, however this is not a solid foundation on which to operate.

As luck would have it, no access to information reports (which have a firm 65 business day deadline) were due during these two periods of Commissioner vacancy; however, in both cases reports were issued shortly before the departure of the Commissioner and new ones were due almost immediately after appointment of a new Commissioner. Although there is an option under section 46(2) to extend the 65 day deadline, that application has to be made by the Commissioner. Such an application could not be made by a staff person who has not been delegated that authority. Without a Commissioner in place, it is questionable whether counsel would have standing to make an application, even if senior staff were to take the risk of attempting to have one filed. Furthermore, an outgoing Commissioner may not have time to make such an application in anticipation of such an issue. Other than past experience, we also have no insight into the length of time the Commissioner's position could be vacant. It is unknown what would happen if a report were due in the absence of a duly appointed Commissioner, however with no one authorized to issue it, it is clear that mischief would likely result that could significantly harm the interests of the parties involved.

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

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

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

As noted above, in both recent cases there has been a vacancy in the Commissioner role for approximately one month. It is our position that there should not be a single business day without an Acting Commissioner in place upon the departure of a Commissioner. Clearly, the administrative processes required to designate a Commissioner, including an Acting Commissioner, require a certain amount of time under the current statutory provisions. Past practice is a reasonably good indication of future expectations, so in our view a legislative solution is required in order to avoid such circumstances.

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

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

> **<u>Recommendation 12.1</u>: Amend *ATIPPA, 2015* to ensure that the position of Commissioner will not be vacant for any period of time, so as to allow the oversight functions of *ATIPPA, 2015* and *PHIA* to continue normally, particularly in circumstances such as the resignation or retirement of a Commissioner, until a new Commissioner is appointed under section 85.**

Access to Information Complaints and Appeals

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

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

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

The circumstance here is not one in which there is a public interest to the extent that section 9(1) comes into play. In weighing the purpose for the exception against the reasons for exercise of discretion, there

are times when public bodies have failed to fully take into account those impacts in comparison with the reason for the exception, and have withheld information when disclosure would cause little if any harm.

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

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

Clarity of Breadth of Applicant's Right of Appeal

It is our view that any time an access to information applicant files a complaint under section 42, there is a clear path through the Commissioner's review process to an appeal at the Trial Division. Section 42 is quite broad in its language – the threshold is that the complaint must be a matter "respecting a decision, act or failure to act of the head of the public body" and it need only "relate to the request" for access or correction. Under *ATIPPA, 2015*, a complainant has two options – they may go to the OIPC, or they may go directly to the Trial Division, where the language in section 52(1) closely mirrors that of section 42.

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

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

getting the records requested, this amounts to a refusal to grant access, and is encompassed within section 54.

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

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

In our view, this is contrary to section 49, which requires the head of the public body to decide whether to follow our recommendations (49(1)(a)) and give written notice of that decision to relevant parties. Section 49(3) specifies the contents of that notice, including the right of appeal. In our view, such an approach to statutory interpretation is not consistent with the purpose of *ATIPPA, 2015* and contrary to the principles of statutory interpretation. Eventually this may have to be addressed by a Court, however this statutory review presents an opportunity to do so that will avoid the cost and delay of a court process for all parties.

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

Disposition of an Appeal

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

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

Ex Parte *Applications for a Declaration under Sections 50 and 79*

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

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

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

Public Body Notification of Applicant on Third Party Appeal

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

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

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

The Applicant is not required to participate in a third party appeal, as the third party bears the burden of proof. The Applicant, therefore, should not be punished for remaining silent and awaiting the outcome. On the other hand, there is a cost to the parties involved to proceed with a review of a third party's appeal when the matter may be moot, if the Applicant is no longer interested in obtaining the records. From the third party's perspective, although it might appear that the Applicant is no longer interested, if the third party withdraws their appeal, that means disclosure of the information is no longer contested, and the public body is obligated to send the information to whatever address for the Applicant is on file. In cases where the email/mailing address/phone number are no longer valid, the risk for the third party may be low; however, in cases where the Applicant has simply chosen to remain silent, third parties are understandably reluctant to simply withdraw.

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

Local Public Bodies and Transparency

Local public bodies are defined in *ATIPPA, 2015* as follows:

> *2(p) "local public body" means*
>
> *(i) an educational body,*
>
> *(ii) a health care body, and*
>
> *(iii) a local government body;*

Local government bodies cover all of the municipalities in the province, including the incorporated cities.

Privileged Meetings

Section 28(1)(c) is the discretionary exception which allows public bodies to withhold the substance of deliberations of its private or privileged meetings, provided that an Act authorizes such meetings:

> *28(1)(c) the substance of deliberations of a meeting of its elected officials or governing body or a committee of its elected officials or governing body, where an Act authorizes the holding of a meeting in the absence of the public.*

There is at present a lack of consistency in terms of the information that is or should be protected from disclosure by this provision, primarily due to the fact that most of the Acts in question are silent in terms of the subject matter that is appropriate for a privileged meeting. Research from other jurisdictions demonstrates that comparable statutes in some cases do actually limit the subject matter of such meetings, and as a result there is greater transparency about the operation of such local public bodies. Amendments to the specific Acts governing these public bodies are the most appropriate means of addressing this issue, however there are some aspects that can be considered in this context.

In particular, section 62(2) of the *Schools Act, 1997* is listed in Schedule A of *ATIPPA, 2015*, which means that it takes precedence over the *ATIPPA, 2015* as a result of section 7(2). Section 28(1)(c) is already available to a school board that wishes to withhold information from minutes or other records of a privileged meeting. Having section 62(2) in Schedule A simply means that there are no limitations on the absolute nature of the prohibition, however it is submitted that section 28(2) *ATIPPA, 2015* would not significantly impair the intended purpose of 62(2).

The *Schools Act, 1997* predates the original *ATIPPA*, which came into force in 2005. Section 62(2) has been one of the provisions listed as taking precedence over the statute ever since that time. It is our view that this may have been included out of an abundance of caution. Schedule A should only list those provisions which are necessary to be included. In our view, section 28(1)(c) accomplishes the same purpose.

> **Recommendation 14.1: Remove section 62(2) from Schedule A as it is redundant to section 28(1)(c).**

Section 12 of the Schools Act, 1997 *and Schedule A*

Another issue relates to the access to the information process, and again implicates Schedule A. The OIPC has issued two reports regarding the interaction between section 12 of the *Schools Act, 1997* and *ATIPPA, 2015*. In both reports, the Commissioner disagreed with the interpretation of the NLESD. From Report A-2018-010:

> *[10] The Schools Act, 1997 restricts access to "student records" to the parent or the student when the student is 19 years of age or older. Section 12(2) of that Act is permissive in the sense that the School District is not required to disclose the entire record upon request to the parent or the student – it simply restricts the parties who "may" review the record. Review of student records occur under the supervision of a person designated by the School District. Interestingly, section 12 is silent on whether, as part of that review, a parent or student may make notes on or take a copy of any portion of the student record.*
>
> *[11] As section 12 of the Schools Act, 1997 is listed in Schedule "A" to the ATIPPA, 2015, it notionally prevails to the extent there is any conflict between it and the ATIPPA, 2015. Much turns on the overlap, if any, between the terms "review" and "access". The word "review" is not defined in the Schools Act, 1997. The word "review" is often limited to a viewing or a visual inspection. Interpreting it in that manner excludes any conflict with the ATIPPA, 2015 as it addresses the ability to access copies of records. While I am inclined to the view that the ATIPPA, 2015 applies unreservedly to "student records", I need not decide the matter conclusively as even if correct, in these circumstances the result would be the same. It warrants noting that the Schools Act, 1997 is rather dated on this topic given that we are now in an age of electronic records while paper records were the standard when it was drafted.*

The same issue was revisited in Report A-2019-008:

> *[34] For the same reasons noted in Report A-2018-010, I see no basis upon which to conclude that a conflict exists between the ATIPPA, 2015 and the Schools Act, 1997 in these circumstances. Section 12 of the Schools Act, 1997 establishes a process, at the discretion of the District, for a parent or student to review the student record in person with NLESD staff, and the NLESD has concluded that the Complainant has already been furnished with the maximum amount of information appropriate to provide him with under that statute. The ATIPPA, 2015 establishes a right of access which includes a right to obtain a copy of a record. That right is abrogated only if an exception applies, and in this case section 40 is a mandatory exception to the right of access which I have concluded applies to the information withheld from the Complainant. As a result, even if I were to determine that a conflict exists, the outcome would be the same for the Complainant.*

In addition to the issue of interpreting whether there is a conflict between the legislative provisions, another feature of Report A-2018-010 is the confusion that was evident during the request process. This legislative review is an opportunity to bring greater clarity for all parties, given that the *Schools Act, 1997* pre-dates the original *ATIPPA* by several years and the language in the two statutes does not align.

The Ontario Information and Privacy Commissioner has come to similar conclusions regarding the interaction of the *Municipal Freedom of Information and Protection of Privacy Act* (*MFIPPA*) and Ontario's *Education Act*, and has issued a guidance document on the subject of access to information pertaining to student records:

> *If a student, or their parent or guardian, wants to access the student's personal information, they might choose to ask for the information informally, by asking the child's teacher for a particular record, for example. If an informal request does not work, or the records are numerous and lengthy, they may choose to make a formal access request. The request can be made under the Education Act or MFIPPA, or both.*

Section 266(3) of Ontario's *Education Act* establishes a right for a student, or his or her parent or guardian where the person is a minor, to "examine" a student record, which appears to be similar to the right to "review" the record provided for in section 12(3) of the *Schools Act, 1997*. Ontario's *MFIPPA* takes precedence over the *Education Act*, therefore, the guidance offered by Ontario's Commissioner is clear and valid, as the *Education Act* offers a right to "examine" a student record while the *MFIPPA* establishes a right to obtain a copy – two separate but related rights which do not conflict.

The *Schools Act, 1997* establishes a right to review a student record only "at a time and with a person designated by the board." It is silent on the right to obtain a copy of a record, however, and that is a right to which the *ATIPPA, 2015* speaks directly. Since the *Schools Act, 1997* came into force, the right of access to records has become well entrenched beginning with the original *ATIPPA* in 2005. Furthermore, the development of electronic forms of communication means that the limitation of reviewing a record in the presence of a board employee appears rather paternal and outdated.

As with Ontario, while section 60 of Prince Edward Island's *Education Act* allows for inspection of student records, the *Education Act* is not listed in the regulations of PEI's *Freedom of Information and Protection of Privacy Act* (*FOIPP*) as taking precedence. Therefore the *FOIPP* access to information process would apply and sit side-by-side with the *Education Act*, one providing for access to a copy of records, including student records, and the other establishing a more informal right to "inspect" a student record.

British Columbia's *School Act* at section 170 makes it clear that the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) is the appropriate forum for access to student records:

> *170(1) A public body as defined in the Freedom of Information and Protection of Privacy Act must not disclose any personal information contained in a student record except for one of the following purposes:*
>
> > *(a) a purpose authorized under the Freedom of Information and Protection of Privacy Act;*
> >
> > *(b) to ensure efficient and effective use of grants paid under sections 114 and 115 of this Act and under sections 12 and 13 of the Independent School Act;*
> >
> > *(c) to evaluate the effectiveness of boards, francophone education authorities and authorities governed by the Independent School Act and the programs, courses and curricula delivered by them.*

Section 9 of British Columbia's *School Act* also provides a right for students and parents to "examine" student records – once again, this right exists in parallel to the right of access under BC's *FIPPA*.

Based on the foregoing analysis, it is therefore recommended to remove the reference to section 12 of the *Schools Act, 1997* from Schedule A of *ATIPPA, 2015* in order to provide greater clarity for those

requesting information pertaining to student records. As noted above, it is the view of the OIPC that there is no conflict between section 12 of the *Schools Act, 1997* and *ATIPPA, 2015*, however the presence of the *Schools Act, 1997* provision in Schedule A of the *ATIPPA, 2015* has created unnecessary confusion. This can be remedied through a simple legislative fix.

> **Recommendation 14.2: Remove the reference to section 12 of the *School's Act, 1997* from Schedule A of *ATIPPA, 2015*.**

Municipal Governments and Privileged Meetings

A further issue related to local public body transparency involves the circumstances under which a municipal government may enter into a privileged meeting. Presently there are no statutory restrictions on this, and there is nothing to keep a municipal governing body from conducting much of its business in terms of debate and discussion about community issues in an opaque forum. This is significant from an *ATIPPA, 2015* perspective because section 28(1)(c) contains a discretionary exception allowing the substance of deliberations of a privileged meeting to be withheld from an applicant. If there are no limits on the purposes for a privileged meeting, this gives municipalities an extremely wide latitude to conduct business in private, impairing the likelihood of accountability through access to information.

Specifically, section 213 of the *Municipalities Act, 1999* allows a council to hold a privileged meeting. Although any decisions taken at that meeting must be ratified at a public meeting, the general public can be left in the dark as to the rationale for those decisions. Sometimes that may be necessary for personnel matters and other appropriate reasons, however the *Municipalities Act, 1999* provides no limitations on the purposes for such private meetings. Similar provisions exist in the *City of Corner Brook Act*, the *City of Mount Pearl Act*, and the *City of St. John's Act*, and none of these specify the purposes for which a privileged meeting may be held.

Ontario's *Municipal Act, 2001* at section 239 governs the conduct of meetings, and it limits the purposes for which a privileged meeting may be held, including labour relations, litigation, etc. There is even, in section 239.1, a provision for an investigation if a municipality is alleged to have contravened these requirements. Nova Scotia's *Municipal Government Act* at section 22 contains similar limitations on the purposes for which a privileged meeting may be held.

Under section 116 of *ATIPPA, 2015*, the Lieutenant-Governor in Council may make recommendations:

> *(f) authorizing, for the purposes of section 28 , a local public body to hold meetings of its elected officials, or of its governing body or a committee of the governing body, to consider specified matters in the absence of the public unless another Act*
>
> > *(i) expressly authorizes the local public body to hold meetings in the absence of the public, and*
> >
> > *(ii) specifies the matters that may be discussed at those meetings;*

The municipal acts in this province, referenced above, do not contain anything which specifies the matters that may be discussed at meetings held in the absence of the public, therefore it would appear that a regulation that specifies these matters could be made.

Recommendation 14.3: Create a regulation under section 116(f) of *ATIPPA, 2015* that specifies the purposes for which a local public body may hold a privileged meeting.

Publication Schemes

Publication schemes were introduced into our legislation in 2015 at the recommendation of the 2014 Statutory Committee, replacing a requirement in the original *ATIPPA* for public bodies designated by regulation to create a "directory of information." The Review Committee defined a publication scheme to be "an outline of the classes of information each public body will publish or intends to publish so it may be read easily by the public" and expressed its believe that the use of publication schemes is the best way to ensure consistent and appropriate publication of information by public bodies."

Section 111 of *ATIPPA, 2015* required this Office to create a template for the publication scheme. This task was completed in January 2016, however a publication scheme has yet to be enacted by government. A draft *Guide to Publication Schemes* was shared with this Office by the ATIPP Office in August 2018, however it has never been put into practice, as no public body has been listed in the regulations for that purpose in accordance with section 111(6).

The 2014 Statutory Review Committee indicated that the Minister responsible for the *Act* should "advise Cabinet to make regulations to specify which public bodies must make their information available and when they should make it available. This would allow a gradual coming into force of the practice of publishing information, with the largest public bodies presumably being able to comply most quickly."

A right of access to information held by public bodies is substantially facilitated when citizens can learn which public body has particular records in its custody. Furthermore, when records are published proactively it can relieve the burden on ATIPP Coordinators to provide access through the formal request process. A functional publication scheme for each public body is therefore an important cornerstone to the right of access.

The template issued by the OIPC discusses each of the required sections of the publication, and offers basic guidance on what information should be contained in each. In accordance with section 111(3) and (4), all public bodies listed in the regulations shall publish:

1. a description of the mandate and functions of the public body and its components;

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

3. the name, title, business address and business telephone number of the head and coordinator of the public body;

4. a description of the manuals used by employees of the public body in administering or carrying out the programs and activities of the public body; and

5. the following information about the personal information banks:

a. its name and location;

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

c. the authority and purposes for collecting the personal information;

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

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

A further, and perhaps less obvious but equally important rationale for a publication scheme is that it requires a public body to conduct and maintain an inventory of the information that it retains, including personal information banks. From a privacy perspective, it become very difficult for a public body to protect and be accountable for the security of personal information if it has no single record listing what information it has, where it is stored and who has access to it.

Sections 10 and 11 of the federal *Privacy Act* deal with personal information banks, and section 10 contains a description of what a "personal information bank" is:

10 (1) The head of a government institution shall cause to be included in personal information banks all personal information under the control of the government institution that

(a) has been used, is being used or is available for use for an administrative purpose; or

(b) is organized or intended to be retrieved by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

A number of statutes across Canada contain provisions similar to section 111. Some focus on personal information only, while others speak more broadly to the creation of a directory of records held by each public body:

- The federal *Access to Information Act* at section 5 requires a publication or bulletin about information holdings;
- Nova Scotia's Act at section 48 calls for the creation of a directory;
- Quebec's law calls for an inventory of personal information files;
- Ontario's law at sections 31, 32 and 33 discusses information to be published or made available as well as a directory of personal information banks at section 44;
- Saskatchewan's Act has a provision which focuses on access to manuals used by public bodies;
- Alberta's law requires at section 87 a directory of records held by public bodies as well as a description of personal information banks;
- British Columbia's law requires a personal information directory at section 69, publication of policy manuals at section 70, and a requirement for public bodies to establish categories of records that are in the custody or under the control of the public body and are available to the public without a request for access;
- Yukon, NWT and Nunavut each call for the creation of a directory.

While Canada's laws call for or appear to require some similar things, one aspect that appears to be missing from all of them is any explicit role for the oversight body to make sure these goals are accomplished. There are statutes in the international context that can help achieve the result that was

clearly intended with the inclusion of section 111 in *ATIPPA, 2015*. For example, Bermuda's *Public Access to Information Act (PATI)* in section 5(1) doesn't look entirely different from section 111:

> *5(1) Every public authority shall prepare an information statement setting out*
>
> > *(a) a description of the structure and organization of the authority and the legislation governing the authority;*
> >
> > *(b) a description of the functions, powers and duties of the authority, including its obligations under this Act;*
> >
> > *(c) a summary of the services that the authority provides, including ongoing programs of the authority;*
> >
> > *(d) a description of all classes of records that are held by the authority, in sufficient detail to facilitate the exercise of the right of access under this Act;*
> >
> > *(e) a description of all manuals used by employees of the authority in administering or carrying out the programs and activities of the authority;*
> >
> > *(f) a description of the policies, rules and guidelines used by the authority to make decisions or recommendations in respect to any person;*
> >
> > *(g) the name and contact information of the person designated by the authority under section 62 as the person to whom requests under this Act may be directed;*
> >
> > *(h) any other information that the head of the authority considers relevant for the purpose of facilitating access by the public to information held by the authority; and*
> >
> > *(i) any other information that may be prescribed.*
>
> *(2) Every public authority shall update its information statement at least once a year, and may do so more frequently.*
>
> *[…]*
>
> *(5) Every public authority shall provide a copy of its information statement, as updated from time to time, to the Commissioner.*
>
> *[…]*
>
> *7(1) The Commissioner may*
>
> > *(a) provide guidance to public authorities with regard to the preparation of information statements under section 5; and*
> >
> > *(b) review the information statement of any public authority to determine if it complies with section 5.*
>
> *(2) Where a public authority has not published an information statement or where the Commissioner determines that an authority's statement does not comply with section 5, the Commissioner may issue an order to the authority requiring it to publish its statement or to bring it into compliance with section 5, as the case may be, within a period to be specified by the Commissioner.*

Although section 5(1) is not very different from *ATIPPA, 2015*'s section 111, there are key differences in the overall publication scheme regime, such as:

- The requirement in 5(2) that it be updated at least annually;
- The requirement to provide a copy to the Commissioner; and
- The role of the Commissioner in section 7 to provide guidance and review, and to order public authorities to publish an information statement if they have not done so.

It is our understanding that this regime is working fairly well. Bermuda's Commissioner has instituted a process of reaching out to each public authority annually to ensure that the information statement has been updated. Generally it has been found to be of assistance to requesters who want to identify which public authority holds records. Even for very small public authorities, it provides an annual touchpoint with *PATI*, and an opportunity for them to consider proactive disclosures to support good governance.

There was a very long delay between passage of *PATI* in the legislature and its coming into force. During this period, it was the Bermuda Government which created a template and required public authorities to complete an information statement. *ATIPPA, 2015* clearly recognized, in section 111(6), that a phased introduction would have practical advantages, however Government has failed to deliver on this. It might be preferable instead to delete such a provision, and instead put in place, in advance, a particular period of delayed proclamation of perhaps one year to allow public bodies to comply.

The *Freedom of Information (Scotland) Act, 2002* also contains prescriptive provisions regarding publication schemes:

> *23 Publication schemes*
>
> *(1) A Scottish public authority must—*
>
> > *(a) adopt and maintain a scheme (in this Act referred to as a "publication scheme") which relates to the publication of information by the authority and is approved by the Commissioner;*
> >
> > *(b) publish information in accordance with that scheme; and*
> >
> > *(c) from time to time review that scheme.*
>
> *(2)A publication scheme must specify—*
>
> > *(a) classes of information which the authority publishes or intends to publish;*
> >
> > *(b) the manner in which information of each class is, or is intended to be, published; and*
> >
> > *(c) whether the published information is, or is intended to be, available to the public free of charge or on payment.*
>
> *(3) In adopting or reviewing its publication scheme the authority must have regard to the public interest in—*
>
> > *(a) allowing public access to information held by it and in particular to information which—*

(i) relates to the provision of services by it, the cost to it of providing them or the standards attained by services so provided; or

(ii) consists of facts, or analyses, on the basis of which decisions of importance to the public have been made by it;

(b) the publication of reasons for decisions made by it.

(4) The authority must publish its publication scheme but may do so in such manner as it thinks fit.

(5) The Commissioner may—

(a) when approving a publication scheme, provide that the approval expires at the end of a specified period; and

(b) at any time give notice to an authority revoking, as from the end of the period of six months beginning at that time, approval of its publication scheme.

(6) The Commissioner, when—

(a) refusing to approve a proposed publication scheme; or

(b) revoking approval of a publication scheme, must state the reason for doing so.

24 Model publication schemes

(1) The Commissioner may, in relation to Scottish public authorities falling within particular classes—

(a) prepare and approve model publication schemes; or

(b) approve such schemes prepared by other persons.

(2) If an authority which falls within the class to which an approved model publication scheme relates adopts that scheme without modification, no further approval of the Commissioner is required so long as that model scheme remains approved; but the approval of the Commissioner is required in relation to any modification of the scheme by an authority.

(3) The Commissioner may—

(a) when approving a model publication scheme, provide that the approval expires at the end of a specified period; and

(b) at any time publish, in such manner as the Commissioner thinks fit, a notice revoking, as from the end of the period of six months beginning at that time, approval of such a scheme.

(4)The Commissioner, when—

(a)refusing to approve—

(i)under subsection (1)(b), a proposed model scheme; or

(ii)any such modification as is mentioned in subsection (2),must state the reason for doing so; or

(b)revoking approval of a model publication scheme, must include in the notice under subsection (3)(b) a statement of the reason for doing so.

Scotland's Information Commissioner's Office, in accordance with statutory requirements, created a Model Publication Scheme which, it is our understanding, has been adopted by all public authorities. Although the statute provides that public bodies may develop their own publication schemes which may be approved by the Commissioner, we understand that this option has not been used.

Both Bermuda's and Scotland's approaches hold distinct advantages over the *ATIPPA, 2015*. The first major advantage is that these provisions are actually in force and working, in contrast to that provided for by *ATIPPA, 2015*. Beyond simply being functional, each also has its own characteristics which should be considered. One characteristic of both is that there was sufficient time built-in to allow for the development of the information statement/publication scheme, and a clear role was built in for the Commissioner to ensure that this was implemented and is maintained.

It has been widely recognized that a provision akin to section 111 has value, as evidenced from its inclusion in so many statutes. In jurisdictions such as Scotland and Bermuda, however, it clearly plays a much bigger role in the access to information system. At a time when public resources are strained, finding a way to lighten the load of ATIPP Coordinators would be a worthwhile endeavour, by making more information proactively available on a routine basis, and furthermore, by informing the public about personal information databases that exist. Make no mistake, however, that this involves an investment of time and effort at the front end, through the creation of a workable publication scheme, which will later pay dividends.

Perhaps the most recent, helpful analysis of compliance with and the effectiveness of publications schemes was produced by British Columbia's Office of the Information and Privacy Commissioner in June, 2020. That report assessed how well section 71 of BC's *FIPPA* was serving its intended purpose, which is to make more information proactively available. Ultimately BC's Commissioner found that compliance with this provision was lacking, and he made the following recommendations:

- All public bodies should establish additional categories of records;
- Categories of records should be published and easily accessible to everyone; and
- Government should update its Open Information and Open Data Policy to include guidance and tools to help ministries identify and establish categories of records for routine release.

From what we have seen, it is clear that publication schemes benefit from specific oversight provisions to ensure compliance. Furthermore, it is also clear that publication schemes will not become a reality if we continue to await a decision from government as to when the first public body will become subject to such a provision. At least in British Columbia the Commissioner is able to say that they are not working as well as they should, however they are far ahead of us in Newfoundland and Labrador, as section 111 is effectively meaningless as long as we continue to see inaction from government regarding section 111(6).

Our recommendations are therefore that:

> **Recommendation 15.1: Section 111(6) should be deleted, and public bodies be given one year from the coming into force of any amendments to *ATIPPA, 2015* to prepare a publication scheme as required in section 111.**
>
> **Recommendation 15.2: A requirement should be added to *ATIPPA, 2015* that public bodies must submit a completed publication scheme to the Commissioner for review and comment prior to that one year period.**
>
> **Recommendation 15.3: The *Act* should be amended to provide the Commissioner with authority to require any deficiencies in the publication scheme to be addressed within a reasonable period of time to be determined by the Commissioner.**
>
> **Recommendation 15.4: The *Act* should be amended to require that publication schemes must be updated at least annually.**
>
> **Recommendation 15.5: All classes of public bodies should be subject to the requirements of section 111, except local government bodies other than the City of Mount Pearl, the City of St. John's, and the City of Corner Brook, and any other public body designated in the regulations as exempt from this requirement on the basis of its small capacity and lack of information holdings.**

Other Minor Improvements to ATIPPA, 2015

The following recommendations are not significant policy issues but, in our view, would improve the operation of the statute. Two of them, however, involve a recommendation to maintain the status quo because, in our view, the Act is operating well.

Definitions

Several definitions in *ATIPPA, 2015* require review to determine whether the current legislation properly encompasses necessary factors or considerations.

Definition of Public Body:

As a result of recommendations in the Green Report, amendments were made to *ATIPPA* to include the House of Assembly and Statutory Offices of the House as public bodies subject to the Act. These are listed in section 2(x)(v). At the same time, an exception was included (currently section 41) which is intended to ensure that the operation of these entities is not impaired by access to information, and that parliamentary privilege is protected. The term "Officer of the House of Assembly" is defined in section 2(s).

Interestingly, while the Green Report recommended the inclusion of these additional bodies as public bodies subject to the *ATIPPA*, the author specifically excluded the Auditor General at that time, and he outlined at page 5-20 his reasons for doing so:

> *The office of the Auditor General should, however, be put in a separate category. At present there is a general obligation of confidentiality imposed on that office by section 21 of the Auditor General Act with respect to matters that come to the staff's knowledge in the course of their work. The Auditor General occupies a special - some would say unique - place in the government. This is cause for proceeding slowly before wrapping this office into any system of general reform of the legislative branch. Having said that, I believe a case can be made for subjecting the Auditor General to basic access to information requirements about the financial and administrative organization of the office. The Auditor General is, by law, an officer of the House and is responsible, just as are other officers, for the expenditure of public money. I am aware, however, that some consideration is being given to making substantial revisions to the Auditor General's constituent legislation. The better approach for the present, therefore, is to exempt the office from the reforms being recommended in this report and to recommend that the application of access to information provisions be considered at the time of the general revision of the Act.*

Given the years that have passed since the issuance of that Report, as well as subsequent amendments to the *Auditor General Act* which were then anticipated, it may be time to consider this issue anew. Whatever amendments have been made to the *Auditor General Act* subsequent to the Green Report, there does not appear to be any special provision in that *Act* which would militate towards or against inclusion of the Auditor General as a public body.

Presently, section 41(c) protects against disclosure of records connected with the investigatory functions of statutory officers of the House of Assembly. Depending on how broadly this is interpreted, an audit would be considered an investigatory function. However, if the Auditor General were to be included, for the sake of clarity it might be preferable to be more specific. The Green Report at page 5-14 cites a paper by Dr. Christopher Dunn:

> *In order to respond to the concerns of the first four offices, the Task Force recommended the exclusion of records connected with the audit or investigatory functions of an Officer of Parliament.*

For greater clarity, if the Auditor General were to be included as a public body subject to *ATIPPA, 2015,* section 41(c) could be amended to say "… records connected with the audit or investigatory functions of the statutory office."

In order to amend *ATIPPA, 2015* to include the Auditor General, sections 2(x)(v) and 41(c) would have to be amended to exclude reference to the *House of Assembly Accountability, Integrity and Administration Act*. That Act excludes the Auditor General from its definition, and that is the means through which the Auditor General is the lone Officer of the House of Assembly that is not a public body subject to *ATIPPA, 2015*. As noted above, section 2(s) already includes the Auditor General within its definition of "officer of the House of Assembly" so there would be no need to include any further description in 2(x)(v) and 41(c) other than Officer of the House of Assembly.

The original decision to make the House of Assembly and statutory officers subject to *ATIPPA* was a reflection of the experience in this province of the House of Assembly spending scandal, as addressed in the Green Report. Not every jurisdiction has been through such an experience. As a result, few jurisdictions include statutory officers as public bodies. Prince Edward Island, Alberta and the federal jurisdiction are the only other examples of statutory officers being fully subject to the access and privacy statute, however in all three, the Auditor General is subject to the law in the same way that other statutory officers are.

> **Recommendation 16.1: Consider whether to expand the scope of *ATIPPA, 2015* to cover the records of the Officer of the Auditor General; if so, for clarity, amend section 41(c) to include audit alongside investigatory functions.**

Definition of Personal Information:

The *ATIPPA, 2015* section 2(u)(iii) refers to "the individual's age, sex, sexual orientation, marital status or family status" as examples of personal information. All human rights statutes across Canada, including section 9 of the *Newfoundland and Labrador Human Rights Act*, have been amended to include gender identity and gender expression, to reflect evolving societal acceptance of the significance of these terms.

Although most statutes use "sex" and "gender" interchangeably, as if the terms are synonyms, modern understanding of these terms reveals that they have different meanings. A recent report prepared for the Government of Canada discussed the collection, use and display of sex and gender information at the federal level, and discussed the difference between the two.[8]

Three privacy statutes that are relatively recent in origin, those in New Brunswick, Nunavut, and Northwest Territories, specifically mention gender as part of either the definition of personal information or in their descriptions of information the disclosure of which would be considered an unreasonable invasion of privacy. Inclusion of "gender" as a separate term in section 2(u)(iii) of *ATIPPA, 2015* would reflect that this is a distinct category of personal information, and furthermore, recognizing it as such in *ATIPPA, 2015* will contribute to a greater reflection of evolving societal norms.

> **Recommendation 16.2: Include gender as a separate term in section 2(u)(iii)**

The Interaction Between ATIPPA, 2015 and Other Processes to Access Public Body Information

Sections 3(3) and 5(2)(a) contain similar provisions that should be reviewed and considered for the purpose of ensuring a user-friendly statute and providing clarity for all who must understand and interpret *ATIPPA, 2015*.

> *3(3) This Act does not replace other procedures for access to information or limit access to information that is not personal information and is available to the public.*

[8] Privy Council Office, 2019, *The Collection, Use and Display of Sex and Gender Information at the Federal Level,* Government of Canada.

[…]

5(2) This Act

> *Is in addition to existing procedures for access to records or information normally available to the public, including a requirement to pay fees.*

These sections have existed together in the statute since the original *ATIPPA* came into force. Similar provisions in other jurisdictions all include either a statement that the acts are "in addition to" or are intended to "complement" other access information processes. It would be preferable to replace the two provisions in our statute with a single provision that retains the principle that while other procedures for access to records or information may continue, the *ATIPPA, 2015* process is an alternative to such processes.

The phrase "in addition to" leads one to view *ATIPPA, 2015* as a parallel option, which we believe is important because other procedures for access could be overly burdensome in terms of time and expense, whereas *ATIPPA, 2015* has legislated timelines, a cost regime, and an appeal process. Conversely, the phrase "does not replace" could be interpreted to mean that *ATIPPA* is not available if another process exists.

For consideration, we offer the following two potential options for *ATIPPA, 2015*:

- (3) This Act is in addition to and does not replace other procedures for access to information or limit access to information that is not personal information and is available to the public.

OR

- (3) This Act is intended to complement and does not replace other procedures for access to information or limit access to information that is not personal information and is available to the public.

The first option may be clearer. It also uses the language, "in addition", that is already in use in s. 5(2).

> **<u>Recommendation 16.3</u> Amend *ATIPPA, 2015* so that there is a single provision containing language regarding the relationship between the access to information process and other processes, to make it clear that while other processes can continue to operate, *ATIPPA, 2015* is always an option.**

Section 4 - *Schedule B – excluded public bodies*

The Commission of Inquiry Respecting the Muskrat Falls Project was added to Schedule B in 2018. The Information and Privacy Commissioner at the time, Donovan Molloy, issued a news release supporting the inclusion of the Inquiry in Schedule B as a temporary measure to allow the work of the Inquiry to proceed effectively and efficiently, on the understanding that all of the records would become subject to *ATIPPA, 2015* after the Inquiry had wrapped up. In Hansard on March 8 Minister Siobhan Coady confirmed this in her remarks respecting the Bill to add the Inquiry to Schedule B: "Following the conclusion of the inquiry, all of this information is subject to the access to information law."

We have been informed that the records of the Muskrat Falls Inquiry have been transferred to the Department of Justice and Public Safety as that Department is responsible for commissions and inquiries. The Department of Industry, Energy, and Technology (Formerly Natural Resources) also retained its own records from the Inquiry.

Given that these records are now in the control / custody of other public bodies and the Inquiry is over, we recommend that *ATIPPA, 2015* be amended to remove the Inquiry from Schedule B.

> **Recommendation 16.4: Amend *ATIPPA, 2015* to remove the Commission of Inquiry Respecting the Muskrat Falls Project from Schedule B.**

Access Request Timelines

The Minister of Justice and Public Safety's Terms of Reference for this Review included a mandate to consider public body response times for access requests and whether the current statutory requirements for response and administrative times are effective. We have completed a jurisdictional scan to assist the Review Committee in this assessment. It is our understanding that 30 calendar days (roughly equivalent to 20 business days) is and has been the standard for many years in Canadian access to information statutes. The term "business day" is defined in section 2(b) of *ATIPPA, 2015* as "a day that is not a Saturday, Sunday or a holiday." The term "holiday" is defined in the *Interpretation Act*.

There are exceptions as indicated below – Quebec appears to have a shorter time period of 20 calendar days, while Nunavut and New Brunswick have longer periods of 25 and 30 business days. We see no need to alter the 20 business day time frame currently in *ATIPPA, 2015*, particularly as there is a time extension process with approval of the Commissioner that in our view is working well for any request that might take longer than 20 business days to respond to. The vast majority of requests for time extensions are met with full or partial approval. Even when a public body is unable to respond within the extended time period we have approved, the OIPC considers subsequent requests for further extension to reflect evolving difficulties with retrieving and reviewing records, unusual volumes of requests being handled at one time, short-term absences of Coordinators due to illness or job vacancies, consulting third parties, difficulty contacting the applicant, etc. The success of our extension process, however, should not be seen as evidence to conclude that public bodies should, again, be permitted authority to determine their own extensions.

Jurisdiction	Section	Time Limit	Comments
Federal *Access to Information Act*	*Notice where access requested* *7 Where access to a record is requested under this Part, the head of the government institution to which the request is made shall, subject to sections 8 and 9, within 30 days after the request is received,* *(a) give written notice to the person who made the request as to whether or not access to the record or a part thereof will be given; and* *(b) if access is to be given, give the person who made the request access to the record or part thereof.*	30 days	Presumed to be calendar days and not business days as the term "business day" is defined and used in other sections.
Federal *Privacy Act*	*14 Where access to personal information is requested under subsection 12(1), the head of the government institution to which the request is made shall, subject to section 15, within thirty days after the request is received,* *(a) give written notice to the individual who made the request as to whether or not access to the information or a part thereof will be given; and* *(b) if access is to be given, give the individual who made the request access to the information or the part thereof.*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
New Brunswick	*11(1) The head of a public body shall respond in writing to a request for access to a record within 30 business days after receiving the request*	30 business days	This would be longer than the norm in the Canadian access to information context.
PEI	*9. Time limit for responding (1) The head of a public body shall respond to a request without undue delay and in any event shall make every reasonable effort to respond to a request not later than 30 days after receiving it unless*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
Quebec	*47. The person in charge must, promptly and not later than twenty days from the date the request was received,*	20 days	Presumed to be calendar days as no mention of "business day" in the Act. This would be shorter than the Canadian norm.

Ontario	*26 Where a person requests access to a record, the head of the institution to which the request is made or if a request is forwarded or transferred under section 25, the head of the institution to which it is forwarded or transferred, shall, subject to sections 27, 28 and 57, within thirty days after the request is received,*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
Manitoba	*11(1)The head of a public body shall make every reasonable effort to respond to a request in writing within 30 days after receiving it unless*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
Saskatchewan	*7(1) Where an application is made pursuant to this Act for access to a record, the head of the government institution to which the application is made shall […]* *(2) The head shall give written notice to the applicant within 30 days after the application is made:*	30 days	The same wording and time frame is included in both The *Freedom of Information and Protection of Privacy Act* and the *Local Authority Freedom of Information and Protection of Privacy Act.* Presumed to be calendar days as no mention of business day in either Act.
Alberta	*11(1) The head of a public body must make every reasonable effort to respond to a request not later than 30 days after receiving it unless …*	30 days	Presumed to be calendar days as no mention of "business days" in the Act.
British Columbia	*7 (1)Subject to this section and sections 23 and 24 (1), the head of a public body must respond not later than 30 days after receiving a request described in section 5 (1).*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
Yukon	*11(1) The records manager must make every reasonable effort to respond without delay and must respond not later than 30 days after a request is received unless the time limit is extended under section 12.*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
Northwest Territories	*8. (1) The head of a public body shall respond to an applicant not later than 30 days after a request is received unless*	30 days	Presumed to be calendar days as no mention of "business day" in the Act.
Nunavut	*8. (1) The head of a public body shall respond to an applicant not later than 25 business days after a request is received unless*	25 business days	This would be longer than the norm in the Canadian access to information context.

<u>Recommendation 16.5</u>: Maintain the current access to information timelines in section 16.

Disregard Timelines

As noted in the introduction to this submission, even though in our view the extension and disregard process works quite well, we do believe that the timeline for a public body to apply for an access request to be disregarded should be increased from 5 to 10 business days. To successfully apply for a disregard, a Coordinator must assess the scope and scale of a request, contact the applicant and actually reach them, and then come to a conclusion that a disregard should be sought. The application for a disregard must be thoroughly substantiated by evidence. There have been several examples where a very lengthy extension is sought for an over-broad request and, when consulted on the matter, the Commissioner has asked why there was not an application for a disregard, only to learn that the Coordinator had run out of time. Applicants may believe that a public body's suggestions to narrow a request are obstructive and this may arise from a lack of awareness of the unreasonableness of an over-broad request. Disregards on overbroad requests, rather than lengthy extensions, may encourage applicants to cooperate with efforts to narrow their requests, leading to faster timelines for the information they really do want. This amendment would also decrease pressure on busy ATIPP Coordinators.

<u>Recommendation 16.6</u>: Amend section 21(1) to increase the timeline for an application to the Commissioner for approval to disregard an access request from 5 to 10 business days.

The Office of the Information and Privacy Commissioner as a Public Body

ATIPPA was amended subsequent to the Green Report to designate the Office of the Information and Privacy Commissioner as a public body subject to the *Act*, along with other statutory offices. We believe that was an appropriate step, and with section 41 having been added at the same time, being a public body has represented no interference with our independent statutory oversight role. Since that time, the OIPC has received 25 access to information requests, all of which have been responded to within 20 business days.

There is, however, one significant issue regarding our position as a public body which we hope to see remedied, which finds us in a unique position among other public bodies. Sections 21 (disregarding a request), 23 (extension of time limit) and 24 (extraordinary circumstances) are necessary and important features of *ATIPPA, 2015* that provide flexibility when difficult requests or other circumstances arise that prevent a public body from complying with the ordinary deadlines and requirements of the *Act*. All of these features require an application to and approval of the Commissioner. However, it is our interpretation that the head of our public body, the Commissioner, cannot apply to themselves for such an approval, and that it would be inappropriate to do so.

Thankfully, to date, there have been no circumstances in which we have received a request that would warrant an application to disregard a request. We have, however, processed one request which was very difficult to complete within the 20 business day statutory time period, and it is conceivable that we could encounter another request that could not be responded to within that period.

In the one challenging circumstance, there were persistent, novel technical issues with conversion of requested electronic documents to a usable format so that all of the information in the record could be accessed for review, redaction, and provision to the applicant. This also involved a large number of records - in excess of 1000 pages. In order to respond by the deadline, this process involved several of our staff who were involved in working through the technical issues, consulting outside the office to find solutions, reviewing the records once the issue was resolved, in addition to applying redactions, communicating with the applicant and other normal administrative processes. Ultimately the response was issued on time, but at the risk of impacting our other statutory responsibilities.

> **<u>Recommendation 16.7</u>: Amend *ATIPPA, 2015* to allow the Commissioner to apply *ex parte* to the Trial Division for approval in regard to sections 21, 23 and 24 in the same way and for the same circumstance that would ordinarily see a public body apply to the Commissioner for such approval.**

Anonymity of Privacy Complainants

Privacy complaints typically fall into two categories. The first, most common one, is when a complainant has been the subject of a specific privacy breach, often the result of a failure of procedure or failure to implement a correct procedure, or a failure to implement appropriate information security, etc. Such complaints may arise from a privacy breach where the individual has been notified, and has been advised of their right to complain to the Commissioner. Sometimes, but not always, the specific circumstances of how the individual's personal information was handled are integral to such an investigation, and in such cases it is not possible for us to investigate, nor is it possible for a public body to respond to our investigation, without the identity of the complainant being known.

Other complaints relate to larger systems. For example, we received a complaint from an individual regarding the Town of Paradise and its implementation of a new video surveillance system. The individual was of the view that the surveillance involved the collection of more personal information than was warranted. In that case, the identity of the complainant was not relevant to our investigation, which was about the surveillance system, rather than about its impacts on the complainant specifically. The complainant provided valid reasons to us why they did not wish to have their name used. We therefore provided the Town with a summary of the privacy complaint, as allowed by section 73(5), leaving out the name of the complainant.

During the complaint investigation process, the Town demanded that we disclose the identity of the complainant. We refused to do so. We then issued Report P-2018-003 recommending that the Town cease collecting personal information via its video surveillance system, which we sent to the Town's designated Head as well as the complainant, in accordance with section 77(1)(b).

The Town was then required, by section 78(b), to give a copy of its response to "a person who was sent a copy of the report." In order to facilitate this, we provided a copy of the Town's response to our Report to the complainant. The Town then filed an application for a declaration under section 79. Again, the requirement for the Town to notify the complainant in section 79(b) conflicted with the complainant's wish to remain anonymous. We therefore took it upon ourselves to make the complainant aware of the declaration application.

Ultimately, the Town provided further information about its surveillance system, and we agreed that if the Town made some specific modifications that we would consent to a Court Order to re-instate its surveillance system, which is how the matter concluded. However, it is clear that the anonymity of the complainant was a sore point for the Town, and was a challenge for us in terms of ensuring that the intent of the *Act* was fulfilled, even though the letter could not be.

That experience taught us that we needed to make it clear upon receipt of a complaint by any complainant who wished to remain anonymous that there could be challenges ahead. Going forward, one option would be to not proceed with the complainant's complaint, but instead initiate an own motion complaint under section 73(3). That might work, however we must consider how that impacts the complainant's experience of pursuing their rights under *ATIPPA, 2015*. It is not an easy matter to carry the weight of a complaint forward, even if you hope to remain anonymous. That being said, a complainant's journey is often founded on personal conviction, and it would be unfair to remove them from the process because of their wish for anonymity where the complainant's identity is not relevant.

However, there is no guarantee, particularly if a matter proceeds to a court process for a declaration application, that anonymity can be retained. While it is incumbent upon us to make complainants aware of such risks, it would also be appropriate to amend *ATIPPA, 2015* so that, in certain circumstances where the identity of the complainant is not relevant to the investigation of the complaint, nor relevant to the public body's ability to respond to that complaint, complainants would more clearly be able to proceed anonymously.

We believe this can be done through the addition of language in Part III, Division 2. Specific language may need to be added to section 73(5) to allow the Commissioner to accept a complaint from someone who does not wish their identity to be shared with the public body, where the complainant's identity is not relevant to the investigation of the allegations. Additional amendments would then be required in sections 77(2), 78(1)(b), and 79(1)(b). We believe that in circumstances where the identity of the complainant is not relevant to the complaint, and the complainant wishes to remain anonymous, that the statute can be amended so that the Commissioner can be required to ensure that the complainant receives a copy of the public body's response to our Report in section 77(2)/78(1)(b), and that we can facilitate service of the application for a declaration on the complainant in 79(b).

> **<u>Recommendation 16.8</u>: Amend *ATIPPA, 2015* to accept a privacy complaint from someone who does not wish their identity to be shared with the public body, where the identity of the complainant is not relevant to the investigation.**

ATIPPA, 2015 and the Evidence Act

The reference in section 101 to section 8.1 of the *Evidence Act* is somewhat obscure and does not arise in day-to-day application of *ATIPPA, 2015*. Section 8.1 of the *Evidence Act* is a provision that specifically prohibits records of quality assurance and similar committees (typically in the context of the health care system) from being produced as evidence in legal proceedings. The intention of section 8.1 appears to be to give medical professionals and their regulatory bodies the freedom to investigate complaints or incidents involving patient safety, with the objective of learning from mistakes and making improvements to medical practice, without risking statements or opinions being used in litigation. In one sense the

purpose of section 8.1 may be analogous to section 29 of *ATIPPA, 2015,* which facilitates the free flow of advice among government officials, allowing frank discussion to occur without fear of disclosure. Without the protection of section 29, officials would be constrained from offering frank advice or addressing controversial subjects.

In section 8.1 "legal proceeding" is defined broadly, and could arguably include an OIPC investigation. The inclusion of section 101, stating that section 8.1 of the *Evidence Act* does not apply to our investigation, means our investigation is not a "legal proceeding" under s.8.1, and that our Office may therefore require the production of the kind of records to which section 8.1 applies, if they are relevant to our investigation.

Importantly, however, it does not mean that such information would necessarily be disclosed to an access to information applicant. The exceptions in Part 1, Division II are available to public bodies that wish to withhold any records subject to an access request.

If further clarity is required, an option might be to amend the existing section 101, or add a paragraph to section 97(1): "(e) notwithstanding section 8.1 of the Evidence Act" to make it clear that s.8.1 does not affect our investigatory powers. This may not be necessary, however, because the entire matter is not a pressing issue. When *ATIPPA* first came into force in 2005 it may have been more relevant, because the *Personal Health Information Act* (*PHIA*) had not yet come into existence. That *Act* was passed in 2008 and proclaimed in 2011, at which point personal health information that had formerly been subject to *ATIPPA, 2015* was now subject to *PHIA*.

Section 58(1)(c) of *PHIA* provides a mandatory exception to the right of access, in summary, for records that are applicable to section 8.1 of the *Evidence Act*. In our view, a similar exception is not necessary for *ATIPPA, 2015* because records of personal health information are already excluded from *ATIPPA, 2015* by section 6. The latter exclusion is likely the reason there has been no application of section 101 over the years, but section 101 may still be necessary to fill the gap that would otherwise exist if our Office were to need to examine records that related to a quality assurance committee, but did not consist wholly of personal health information.

Recommendation 16.9: No amendment is required to section 101.

Appendix A - List of Recommendations

Appendix B – OIPC Comments on the Mandate of the Statutory Review Committee

This appendix is a consolidation of OIPC comments on elements of the mandate provided for the Statutory Review Committee by the Department of Justice and Public Safety.

Public and public body experience in using and administering the ATIPPA, 2015 to access information in the custody or control of public bodies in Newfoundland and Labrador and opportunities for improvement;

> We are interested in the views of the public and public bodies on this question. One caution is that the public and public bodies have very different interests in this matter, and public bodies are much more knowledgeable and well-resourced in terms of their abilities to put forward views on this subject. We urge the Chair to consider the fact that if public input is found lacking, it may be an expression that they are satisfied with how the Act is working, rather than a lack of interest. The continuing increase in the number of access to information requests is a good indication of this, and also the fact that in Newfoundland and Labrador, the vast majority of requesters are individual members of the public.

Whether there are any categories or types of information (personal information or otherwise) that require greater protection than the ATIPPA, 2015 currently provides;

> We have addressed this in our submission in our commentary on artificial intelligence (AI) and biometrics. Although biometrics is about a category or type of information, AI brings a number of other considerations into play, such as opacity of process, the ability to derive insights and knowledge from disparate data points which can create new personal information about an individual; the fact that there are data ethics issues arising from AI which may not exist in traditional collections, uses and disclosures.

Public body response times for access requests and whether the current ATIPPA, 2015 requirements for response and administrative times are effective;

> The 20 business day response time is very much the standard in Canada, and there is no reason to alter it. There is an extension process that works well, and because it involves the Commissioner's Office, unlike the earliest ATIPPA extension model which allowed public bodies to grant themselves extensions, it has a built-in accountability. Our Annual Report statistics show that the vast majority of extensions are either fully or partially granted. Our goal is to ensure that public bodies have reasonable time periods within which to do their work, while ensuring that extensions are only granted when necessary and to the extent necessary to reflect the rights-based nature of the statute.

An examination of exceptions to access as set out in Part II, Division 2 of the Act:

> In our view the 2014 Statutory Review of ATIPPA conducted a comprehensive review of exceptions, and in cases where the exceptions changed as a result of that review to narrow the scope of an exception, it was essentially a change from one model that is found in some

jurisdictions to another model that is found in other jurisdictions. The exceptions that are present in *ATIPPA, 2015* are fairly standard; they have allowed public bodies to function effectively over the past five years, just as they have allowed public bodies to function in other jurisdictions that have the same versions of those exceptions.

The primary exception to this is section 33, on which we have provided significant commentary.

Whether there are any additional uses or disclosures of personal information that should be permitted under the Act:

This would be best put to heads of public bodies and government policy-makers, however we would appreciate an opportunity to respond to any proposals for additional uses or disclosures of personal information.

An examination of the complaints process to the Office of the Information and Privacy Commissioner:

We are happy to submit to an examination of the complaints process at our Office. It is our view that the complaints process under *ATIPPA, 2015* is one of the best in Canada, if not the world, due to the statutory process in place. Other jurisdictions contact us from time to time wishing to learn from us. While we believe we also have effective and efficient internal processes to ensure that we comply with our statutory timelines, our message to most jurisdictions is that encouraging statutory reform similar to what we have in *ATIPPA, 2015* is the best advice we can give.

An examination of the request for extensions/disregards process to the Office of the Information and Privacy Commissioner:

Again, we are happy to submit to an examination of our process in this regard. We believe it works well, as noted above regarding extensions. We have found, however, that the five day period within which public bodies must apply for approval to disregard a request is at times too short. Some public bodies have missed this time frame, and have not been able to establish any extraordinary circumstances to justify a decision to extend that time period. It may be appropriate to consider extending that application period to 10 business days. See recommendation 16.6.

Whether the current Cost Schedule set in accordance with subsection 25(6) of ATIPPA, 2015 is effective:

The issue of costs was examined in the last statutory review, and we believe overall a good balance was struck. There are some procedural challenges that should be assessed, but overall, we are of the view that costs for access to information should be minimal, given the purpose of the statute. Some have argued that certain individual applicants abuse the system by filing requests for large volumes of records, and that this should be deterred through amendments to the cost provision. Our view is that certain requesters may indeed overburden some public bodies, but we need to be careful not to design the statute around exceptional users rather than the average user, and that we do not penalize the average user, who might file one or two requests in their life time, even if one of them is a large request.

Whether there are any entities which would not appear to meet the definition of "public body" but which should be subject to the ATIPPA, 2015:

The last statutory review brought large public entities such as St. John's Sports and Entertainment, Metrobus, and the Regional Service Boards under the definition of "public body", which was a very positive step. We have no recommendations to make on this issue at present.

Whether the provisions of the ATIPPA, 2015 are effective for local government bodies:

We have made specific recommendations in this Report regarding local public bodies, of which local government bodies are a subset. Please see recommendations 14.3 and 16.10.

Consideration of Recommendations 3, 4, and 16 arising from the Report issued by the Honourable Richard D. LeBlanc, Commissioner of the Commission of Inquiry Respecting the Muskrat Falls Project, dated March 5, 2020, and report on conclusions with respect to those recommendations:

Muskrat Falls Inquiry Recommendation 3: Based on this and other recommendations, Commissioner LeBlanc clearly understood that the lack of transparency in the Muskrat Falls Project was directly connected to the failure of oversight and accountability. It is not clear, however, whether this particular recommendation will yield the intended result of opening Nalcor to sufficient scrutiny to prevent such failures in the future. Perhaps one of the biggest stumbling blocks here is the definition of "commercial sensitivity" in the *Energy Corporation Act*. In any other context, contracts entered into by a public body would be public. In any other context, the threshold to withhold third party business information would be section 39, and section 35 would serve to protect public body commercial or financial information. In our view, it has never been adequately explained why the *ATIPPA, 2015* regime would not work for Nalcor. Sections 35 and 39 also protect commercially sensitive information, but they do so to the extent necessary. In our view, the definition and the construction of section 5.4 in the *Energy Corporation Act* cast an unnecessarily broad net over the information held by Nalcor.

In our submission to the 2014 Statutory Review of ATIPPA we pointed out that Manitoba Hydro is a crown corporation that is subject to the *Freedom of Information and Protection of Privacy Act* (*FIPPA*) in that province. It undertakes much the same kind of work in developing major hydroelectric projects as Nalcor has done, yet it operates within *FIPPA* in the same manner as any other public body.

Beyond the breadth of the definition, the main issue is with section 5.4. It already says that the Commissioner can determine whether the information is commercially sensitive, but the process is unlike that found in *ATIPPA, 2015*, and lacks clarity. It is arguable that 5.4(2)(a) and (b) constitute the threshold necessary for such a determination by the Commissioner, otherwise it is difficult to see why the certification and confirmation process is present. Normally, under *ATIPPA, 2015*, when the head of a public body refuses access based on an exception, there are no certificates involved. A decision has been made, and we review that decision if a complaint is received. If we are intended to review and make a determination based on argument and evidence presented by Nalcor whether or not the exception applies, then the certification and confirmation process is unnecessary.

<u>Recommendation 17.1:</u> Amend section 5.4 of the *Energy Corporation Act* to remove the certification and confirmation process to make it clear that the Commissioner's review of a decision to deny access places the burden of proof on Nalcor, and it must discharge that burden through the presentation of evidence and argument about commercial sensitivity and the expected harm from disclosure, as would be the process for any other public body under *ATIPPA, 2015* and remove section 5.4 of the *Energy Corporation Act* from Schedule A of *ATIPPA, 2015*.

<u>Recommendation 17.2:</u> Remove from Schedule A and make corresponding amendments to the *Innovation and Business Investment Corporation Act* and the *Oil and Gas Corporation Act*, both of which, while less well known, contain a very similar statutory scheme to the *Energy Corporation Act*. We detailed our concerns about both in our *2018-2019 Annual Report*.

<u>Muskrat Falls Inquiry Recommendation 4</u>: The first part of this recommendation is that Nalcor should not be entitled to withhold information from the Premier, the Minister of Natural Resources, the Minister of Finance or the Clerk of the Executive Council on the grounds of legal privilege or commercial sensitivity. Broadly speaking, we are in favour of ensuring sufficient oversight of megaprojects in order to prevent "boondoggles", however *ATIPPA, 2015* would not normally be the relevant statutory framework for determining what information one public body can or cannot obtain from another if the information is not personal information. As for the second part of the recommendation, it is our belief that the persons holding the positions noted above are already only able to withhold such information from public disclosure under the *Energy Corporation Act* and/or *ATIPPA, 2015* providing a request for access is received and the information is in their control or custody. In the absence of a request for access to information, however, the disclosure of non-personal information in the control or custody of a public body is at the discretion of the head of that public body. If those public bodies enter into contractual arrangements preventing such disclosure, such contractual arrangements do not override the statute in the event of an ATIPP request.

<u>Recommendation 17.3</u>: Address Recommendation 4 of the Report of the Muskrat Falls Inquiry through means other than an amendment to *ATIPPA, 2015*.

<u>Muskrat Falls Inquiry Recommendation 16</u>: Commissioner LeBlanc recommended that a Duty to Document be legislated, and that this apply to crown corporations and agencies as well. We agree with this recommendation, and have presented our views in the body of this submission. See Recommendation 3.1.

Appendix C – Letter from Commissioner Harvey to Commissioner LeBlanc

OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

November 4, 2019

BY EMAIL

The Honourable Justice Richard LeBlanc
Commission of Inquiry Respecting the Muskrat Falls Project
5th Floor, Suite 502
Beothuck Building
20 Crosbie Place
St. John's, NL A1B 3Y8

Dear Commissioner LeBlanc:

Subject: Duty to Document

I am writing at this time concerning the topics of the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA,* 2015) and the Duty to Document (D2D) that arose during the end of the hearings of the Commission of Inquiry Respecting the Muskrat Falls Project (Muskrat Falls Inquiry). As I had not been appointed as the Information and Privacy Commissioner until August 5, I did not have an opportunity to express my views at the time. Now having served some time in this capacity, and having had the opportunity to reflect on this role as well as my previous roles and consult with officials in the Office, I have formed some opinions and perspectives that I believe could be helpful as you form any recommendations you might offer regarding these topics.

I understand that the time for submissions has passed and that you are well into the process of writing your report. Nevertheless, it is my hope that you may be willing to consider these comments.

I can offer a unique perspective on access to information and the D2D. Prior to my appointment as Commissioner, I spent 10 years at the senior management level in the provincial public service, including seven years in executive roles, in a mix of central agency and line department roles. I served as Executive Director in Cabinet Secretariat from spring 2012 through summer 2015. At the tail end of that time, I was assigned to lead the government-wide change management associated with the implementation of *ATIPPA, 2015*. In this capacity, I supported the Minister of the day as the bill proceeded through the House of Assembly and worked with executive across government and external public bodies to prepare them for the cultural change that would be necessary for its implementation. Then, as Assistant Deputy Minister (ADM) in the Department of Health and

P. O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 • Facsimile: (709) 729-6500
E-mail: commissioner@oipc.nl.ca • www.oipc.nl.ca

Community Services, one of the departments with the largest volume of access for information requests, I became directly involved in the *ATIPPA, 2015* process including eventually becoming the executive process owner as the ADM responsible for information management.

My experience in these roles led me to be concerned with some of the sentiments I heard expressed during testimony at the Inquiry regarding *ATIPPA, 2015* and the D2D. In particular, my predecessor, now-Justice Donovan Molloy expressed concerns about a "chilling effect" of *ATIPPA, 2015* whereby senior government officials were less likely to document their decision-making for fear of those documents making their way into the public domain or alternatively, facing some sort of punishment, for having created such documents. Professor Kelly Blidook also, in his report to the Inquiry, reported that many among his senior government official respondents felt similarly. While I do not entirely disagree with these sentiments, my concern is that one might draw the conclusion, erroneous in my view, that the appropriate response might be to tighten the public's access to information in the upcoming statutory review of *ATIPPA, 2015* in order to provide public servants with more protection to share their views candidly, objectively and in writing.

First, and most importantly, *ATIPPA, 2015* may be the most progressive access to information and protection of privacy statutes in the country. It strikes an excellent balance between the public's right to access and the exceptions to access that protect public bodies' responsibilities to govern and operate. The hybrid ombud/order-making authority that it confers upon me as Commissioner is well suited for a small jurisdiction such as Newfoundland and Labrador. In consequence, citizens in this province are now getting more information from their public bodies than most of their counterparts elsewhere in the country, and in most instances they are getting it faster and for free. The intervening years since implementation of the Act have demonstrated that certain amendments may be beneficial, and my Office has been preparing to make a submission during the scheduled 2020 statutory review; however, in our view the Act is fundamentally sound, we are lucky to have it, and we should be very careful not to undermine its core principles.

If the concern that has emerged during the Inquiry is that documentation was lacking, which might have helped understand certain decisions regarding Muskrat Falls, then I reiterate my plea that restricting access to information legislation would be the improper remedy. It may indeed be the case that were there a statutory D2D and a more restrictive *ATIPPA*, there would be more documentary evidence available to the Inquiry. If so, this information would only be helpful for accountability purposes during a judicial inquiry or some other extraordinary process whereby production of such documents could be compelled, rather than readily available to the public on a regular basis as under *ATIPPA, 2015*. While better documentation is intrinsically good as it makes for better decision-making, it does not improve accountability if the public cannot access these documents, (subject of course to the exception provisions of the ATIPPA).

Conversely, I believe that to operate properly, a truly effective access to information statutory regime *require*s a statutory D2D. This is not a novel view. Canada's Information and Privacy Commissioners expressed it in a 2014 joint resolution of which my predecessor

was a signatory. The OIPC expressed this view to the 2014 Statutory Review Committee of the *Access to Information and Protection of Privacy Act* in 2014. As the Committee pithily put it in its report: "how can Information and Privacy Commissioners properly oversee access to information and privacy law in the absence of good records or, in some cases, no records at all?" As you are aware, these observations informed the Committee's recommendation that a D2D be imposed through the *Management of Information Act* (*MOIA*), subject to oversight by the OIPC, and supported by resources to public bodies developed by the Office of the Chief Information Officer (OCIO).

Proper information management practices are central to better public administration. A minister briefed on the basis of good documentation makes better decisions not only because a decision for which she is more easily held accountable is more likely to be a fair one, and thus a better one, but she is better informed in making her decision. The principles of natural justice and procedural fairness tell us that a decision supported by clear and written reasons is more likely to be fair, just and better. Some of Professor Blidook's respondents expressed concerns that accountability was undermined when ministerial briefings were not properly documented. I can personally attest that such meetings, while not the norm, were also not uncommon during my time in the provincial government and that wariness of access to information was one reason for that. I have been similarly concerned that poor documentation practices lead to poor operationalization by public bodies. It is certainly not uncommon in the provincial public service (and, to be fair, certainly in almost every organization in the world) for a course of action to be decided at a non-minuted meeting one week, only to reconvene the following week for participants to discover incomplete tasks because they had not been captured, communicated or understood. It was Max Weber's concern for military-inspired operational efficiency that led him to include formal rules-based processes at the heart of his bureaucratic principles. In short, in my view, the D2D, alongside an effective access to information regime, is central not only to improving democratic accountability but also to improving sound public policy-making and the delivery of public goods and services.

I believe that the demand for a statutory D2D in Newfoundland and Labrador is presently acute, driven by a number of trends that have emerged over the past fifteen years. However, I have also observed a number of trends that, in my opinion, set the stage for the successful implementation of a statutory D2D.

I started my career in the provincial public service in 2006 in the Intergovernmental Affairs Secretariat at a time when *ATIPPA* was a new statute. Intergovernmental officials were aware of *ATIPPA* but also aware of the exceptions in the Act related to matters harmful to intergovernmental relations and policy advice, among others, that were designed to, and were effective in, allowing us to provide our advice to our principals. Concisely and clearly providing both advice and information in written documentation, and preserving that documentation effectively while disposing of unnecessary transitory records was the clear direction from the deputy ministers in the Secretariat at that time (2006-2011). Added to my later experience in Cabinet Secretariat, I came to understand that the culture of central government during this period and prior to it was a traditional, paper- and rules-based

approach to information management. I don't believe that the impetus was accountability or transparency; indeed another principle – *secrecy* – was paramount. But these principles were seen to support sound decision-making and the outcome at that time was good information management.

While these principles formed the dominant culture of Executive Council and certain other key departments at the core of government, they were not universal within the provincial government. In a number of line departments with which I interacted with during my time in Executive Council, information management systems were often rudimentary. As for the departments in which I worked, both Children, Youth and Family Services and Health and Community Services had highly prioritized improving their information management systems during the periods I spent there (2011-2012 and 2015-2019 respectively) but both were dealing with challenging information management legacies.

A number of factors started to combine in the late 2000s that disrupted the above-referenced principles of information management. Resistance in the context of the full implementation of *ATIPPA* was certainly a contributing factor. In my opinion, response from within the public service to this new legislation variously arose from the cultural principle of secrecy, or the challenges of implementation in a context of poor documentation, or both. As noted, I do not entirely disagree with my predecessor or Prof. Blidook's respondents that there was a "chilling effect" that came along with *ATIPPA*. However, I think that other factors were even more disruptive – technology and generational change within the public service.

The availability of electronic communication and the generational change within the public service of staff who could and would comfortably use it, rather than traditional paper-based memo correspondence, dramatically increased the *supply* of information. There are now dramatically more documents created within public bodies than previous. I am far from the first to make this observation, but I make it to note another less-remarked upon: that the low resource cost of communication also increased the *demand* for information. Twenty years ago, in receipt of a document as part of the decision-making process, and faced with a question about it, a senior public servant or Minister might have chosen to send the document back for revision. Asking for a new draft would be time consuming and uncertain, and so the reader would tend to be judicious with his questions and would leave some to go unasked when approving the document to continue in the process. But the advent of, email allowed any and all questions to be asked *immediately*. Technology savvy-staff were increasingly comfortable with word processing and email, editing their own documents without administrative support, and answering questions often with the sole support of Google. Increasingly, therefore, answers could be expected along similar timeframes. Moreover, aware of this, principals began to expect that such documents can be prepared *now*. A Cabinet submission which once would have been reviewed within Executive Council and generated a page of questions now will often trigger a week's worth of emails between a Cabinet Officer and officials in a dozen departments, resulting in the creation of hundreds of records. The implications for the quality of those documents, and the information and accuracy of the information within, are obvious.

There is little question that the information age has contributed to our access to information with immense benefits to how well we can understand our world, but the demand for this understanding to be immediate has undermined many of those gains. The consequence has been a dramatic proliferation of documents of questionable quality – a steadily deteriorating signal-to-noise ratio. For any set of records, the truly valuable information and analysis supporting sound decision-making and operationalization and supporting transparency and accountability (i.e. the signal) is increasingly drowned out by unnecessary, often ill-thought-out and even inaccurate questions, information and analysis, (i.e. the noise) that would not have been produced if the face-value cost of doing this work did not seem so low because of the ease of email. My Office recently received a request for a time extension under section 23(1) of *ATIPPA, 2015* from a department related to a single, relatively mundane issue within a limited timeframe, for which there were 4,000 responsive records. We had little choice but to approve the extension out of consideration for the overworked Access and Privacy Coordinator tasked with responding to the request. However, I knew when authorizing it that not only would the applicant's right to access be compromised by the delay, but that when the records were ultimately provided, most would be of very limited value. At the same time, I also despaired of the departmental person-hours spent on producing these thousands of records in the first place and whether the noise itself compromised the integrity of the signal.

While the above trends cause concern and demonstrate the need for change, there are three ongoing positive trends that, in my view, have set the stage for a statutory D2D. In each case, these positive trends are responses to concerns highlighted above: progress on cultural change; the positive promise of technology; and increasingly consistent sophistication in information management.

First, in my view, the public sector in this province is undergoing cultural change that was initiated by the implementation of *ATIPPA, 2015*. The work and report of the 2014 Statutory Review Committee, the Bill that it produced, and the Act that was passed by the House of Assembly, identified and addressed many of the problems that the Government had been facing with transparency and accountability. By this point, all political actors had come to understand the public's visceral response to the regressive elements of Bill 29 and their political consequences. The universal acceptance of the core principles of *ATIPPA, 2015* by the political leaders of the day was clear direction to the public service. A strong message was sent to the public service by the Clerk of the Executive Council, in appointing a change management team led by an executive from her office, that these principles were to be incorporated into departmental realities. While this cultural change was initiated long after the Muskrat Falls Project had been sanctioned and achieved financial close, in my view and experience, it has indeed been initiated. In certain departments, and I can speak specifically about the department in which I worked, Health and Community Services, the shift towards openness progressed smoothly over the subsequent four years. I can also attest that attitudes within Cabinet Secretariat itself towards secrecy have also begun to change, with a shift from a focus on secrecy as an almost sacred and overriding concept, to a more mature and informed view of secrecy as it appropriately informs the constitutional principle of cabinet confidentiality. There is little question that the cultural change still has a way to go.

For example, the performance of Government on proactive disclosure, for example, has been disappointing. It has also been uneven. In my view there are certain departments, which I will not identify for the sake of discretion, which have not embraced the principles of openness as clearly as others due in roughly equal parts to institutional culture and the attitudes of their deputy ministers. That said, I am confident that change is occurring and the introduction of a statutory D2D at this juncture will only further support that change.

The second supportive trend is technology which, while contributing to the problem, also can help solve it. Every department in the provincial government now has implemented Hewlett Packard's Records Management (HPRM, formerly known as TRIM) and the Office of the Chief Information Officer (OCIO) provides support to the TRIM Administrators Group community of practice. The way in which HPRM is implemented in government department varies depending on the business needs of the department, its capacity, and its maturity, but as a centrally-supported enterprise solution, HRPM provides a core information management system to support the essential functioning of a D2D within core government. I am confident that major public bodies that would be covered by a D2D either already have or could, before long, implement a similar records management system to support them. Increasingly staff at all levels of public bodies in the province are sufficiently proficient with technology to effectively utilize these tools in a way that makes sense for their operations.

Finally, a third supportive trend is an increase in the consistency in information management across public bodies. While, as noted above, in the late 2000s and early part of the present decade there was a sharp difference between the formal and rigid information management systems of central government and the less coherent systems of many line departments, a significant amount of work by line departments and OCIO has increased the consistency of sophistication across the provincial government. Beyond supporting the many instances of HPRM/TRIM, OCIO has developed for, and supported the implementation by, public bodies of various guidelines, frameworks, policies and tools. These include guidelines on IM governance framework and program plans and tools such as the Information Management Capacity Assessment Tool (IMCAT) and the Information Management Self-Assessment Tool (IMSAT). While OCIO's leadership and work in this regard have been essential, at the same time departments and many other public bodies have been increasing the sophistication of their information management systems for their own business needs as they execute Government's policy priorities. There is little question that the level of sophistication will vary, particularly among small agencies, boards and commissions with limited capacity; however, there is little question that the trend is towards an increase in sophistication.

If the need is clear and the stage is set for a statutory D2D, what would this look like? To answer this question I largely draw on the work and recommendations of David Loukidelis, the former Information and Privacy Commissioner for British Columbia, as well as its former Deputy Minister of Justice and Attorney General. Then-Commissioner Loukidelis wrote a report on the D2D, the recommendations of which led to the introduction of statutory provisions in the *Information Management (Documenting Government Decisions) Amendment Act, 2017*. Mr. Loukidelis defines a D2D as "a legal duty requiring public

servants to adequately document specified decisions and actions". One concern that he addresses, to which I am very sensitive, involves the risk that an improperly conceived D2D may lead to the over-documentation of trivial matters. Indeed, I think that at present, trivial matters are entirely over-documented because of the ease of email communication and poor records management which leads to the improper retention of unnecessary transitory emails. This approach undermines access by exacerbating the above-noted signal-to-noise ratio and impedes sound public administration. A sound approach to D2D would provide direction on both what to record and what not to record, in the first place, and what to retain and not to retain, for the record. To achieve that, considering the diversity of public bodies in the province, an appropriate statutory D2D should be pitched at the level of principles. It should support, enable and mandate the development of specific D2D policies and procedures at the entity level, customized to the business needs of each entity. Design should be local, within an overarching policy framework.

This should involve:

- Each entity to which the statutory provision applies must be directed to adequately document decisions and actions.
- Direction must be provided to entities regarding the considerations to be applied in deciding what to document, including contextual factors such as the entity's mandate, legal framework, operations and implications for access to information and privacy.
- Legislation should delegate entities the authority to decide what to document and how.
- Each entity should be required to designate a responsible authority.
- Legislation should establish oversight by a central expert authority.

These are the principles that, broadly, inform British Columbia's statute. However, there is one matter in which my opinion differs from that of Mr. Loukidelis. He recommends that the central duty to document policy should be under the purview of the chief archivist or government records officer and I agree with him on this point. In this jurisdiction this role would be best performed by the OCIO. However, he views that monitoring and audit would also be best performed by this body. In the present BC statute, accountability for oversight rests with the responsible Minister via a chief records offer. The present Information and Privacy Commissioner for British Columbia has noted that the implication is that the Minister is responsible for investigating his or her own conduct and has called for oversight to be placed with the Office of the Information and Privacy Commissioner. I concur with this approach which, I note, is that recommended by the 2014 Statutory Review Committee. While the OCIO is well-positioned to be responsible for the policies, programs and other supports for public bodies, true oversight to engender the public trust requires the independence of a statutory officer of the House of Assembly. The discussion and debate around this matter during the Muskrat Falls Inquiry illustrates that there has been damage to the public trust that public bodies properly document their decisions. I am sensitive to potential criticisms that the assessment of D2D requires as much expertise in the principles

of information management and operationalization of programs and services as it does expertise in the area of access to information. Although some additional resources would be required, if responsibility for oversight was provided to the OIPC, I believe that the staff complement at present would be an excellent foundation on which such additional capacity could be built. OIPC staff deal with access and privacy complaints from the enormous variety of public bodies in the province on all manner of issues and through this have been exposed to the full range of government documents in every sector, as well as to some of the information management challenges that are sometimes at the root of access to information complaints.

As an aside, I should also note that instituting a D2D in this province is not wholly virgin territory. On December 17, 2017 the House of Assembly passed the following amendments to the *House of Assembly Accountability, Integrity and Administration Act*:

> *21.1 The commission, officers and staff of the House of Assembly service shall be responsible and accountable for ensuring that all advice, deliberations, decisions and recommendations of the commission that result from formal or informal meetings of the members of the commission are properly documented in accordance with the Records Management Policy of the House of Assembly.*
>
> *[...]*
>
> *66. (1) A person who fails to comply with section 21.1 is guilty of an offence.*
>
> *(2) A person having a duty to document decisions and maintain records of the commission, the speaker, the clerk or staff member of the House of Assembly service and a person who without lawful authority destroys documentation recording decisions of the commission, the speaker or the clerk, or the advice and deliberations leading up to those decisions, is guilty of an offence.*
>
> *(3) A person who is guilty of an offence under subsection (1) or (2) is liable on summary conviction to a fine of not more than $10,000 or to imprisonment up to 6 months.*

In speaking to the bill in the legislature, Minister Andrew Parsons referred back to the Green Report, which was the genesis for that Act. In his Report "Rebuilding Confidence: Report of the Review Commission on Constituency Allowances and Related Matters" Commissioner Hon. J. Derek Green refers back to the federal Gomery Inquiry in discussing the D2D, and at recommendation 9 at page 5-24 Green explicitly recommends a D2D as well as the creation of an offence for failure to do so. Apparently it took some time before this particular recommendation was fulfilled.

To conclude, I wish to reiterate that if there has been a "chilling effect" arising from *ATIPPA* since its first incarnation in 2005, then I urge you against concluding that an appropriate response might be to restrict that statute's application. We have come too far. Instead, as

has been recognized nationally and internationally, the implementation of a statutory D2D can address that problem by providing public servants with the legal authority they can use to resist the pressure to *not* document properly. At the same time, a properly designed D2D can support sound public administration in the context of a rapidly changing technological environment and public sector culture. In this province, recent developments not only make the need for such a requirement acute, but the conditions are right for this province to be leaders nationally in this area in the same way that four years ago *ATIPPA, 2015* established us as leaders in the area of access and privacy.

Again, I appreciate that your ability to consider my views in the development of your report and recommendations may be limited, but I appreciate any consideration that you may be able to give them.

Yours sincerely,

Michael Harvey
Information and Privacy Commissioner

Appendix D – Examples of Definitions of Common and Integrated Program in Canadian Legislation

Schedule 1 of British Columbia's *Freedom of Information and Protection of Privacy Act* states:

> *"common or integrated program or service" means a program or service that*
>
> > *a) provides one or more services through*
> >
> > *(i) a public body and one or more other public bodies or agencies working collaboratively, or*
> >
> > *(ii) one public body working on behalf of one or more other public bodies or agencies*

New Brunswick's *Right to Information and Protection of Privacy Act* has a definition and an interpretation of the definition:

> *"common or integrated service, program or activity" means a service, program or activity that is provided by*
>
> > *(a) a public body and one or more other public bodies or one or more non-public bodies, or*
> >
> > *(b) a public body on behalf of one or more public bodies.*
>
> *Interpretation of the definition "common or integrated service, program or activity"*
>
> *1.1(1)For the purposes of the definition "common or integrated service, program or activity", a public body or non-public body shall be deemed to be providing a service, program or activity if that public body or non-public body discloses personal information that relates directly to and is necessary for the provision of the service, program or activity by another public body or non-public body.*
>
> *1.1(2)The disclosure of personal information referred to in subsection (1) may occur one or more times or on an on-going basis.*

Saskatchewan's *Freedom of Information and Protection of Privacy Act Regulations* defines "common or integrated service" in section 17.1.

> *17.1(1) In this section: (a) "common or integrated service" means a program or activity designed to benefit the health, safety, welfare or social well-being of an individual that is delivered by a government institution and one or more of the following:*
>
> > *(i) another government institution;*
> >
> > *(ii) a local authority;*
> >
> > *(iii) a trustee as defined in The Health Information Protection Act;*
> >
> > *(iv) a First Nation;*
> >
> > *(v) a police service or regional police service as defined in The Police Act, 1990;*
> >
> > *(vi) the Royal Canadian Mounted Police;*

(vii) a non-profit organization that provides a service of the type to be included in the common or integrated service;

(viii) any other agency or organization that the minister determines is appropriate;

Although passed by the legislature but not yet proclaimed in force, the Northwest Territories Bill 29 *An Act to Amend the Access to Information and Protection fo Privacy Act* adds a definition to section 2:

> *"common or integrated program or service" means a program or service that provides one or more services through a public body working collaboratively with one or more other public bodies, or with an agency or a combination of public bodies and agencies;*

Appendix E – Legislative Language Regarding Information Sharing Agreements

BC's *Freedom of Information and Protection of Privacy Regulations* establishes the requirement for written documentation for common or integrated programs or activities, stating in section 12:

> *12 The written documentation that confirms that a program or activity is a common or integrated program or activity is*
>
> *(a) a written agreement that*
>
> *(i) is signed by the head of each public body and agency through which, or on whose behalf, as applicable, the services of the program or activity are provided, and*
>
> *(ii) includes the following information:*
>
> *(A) a description of the services provided by the program or activity;*
>
> *(B) a description of the types of personal information collected, used and disclosed in the course of providing the program or activity;*
>
> *(C) a description of the purposes, key objectives and expected benefits or outcomes of the program or activity;*
>
> *(D) a description of the respective roles and responsibilities of each public body and agency through which, or on whose behalf, the services are provided;*
>
> *(E) the date on which the program or activity will start and, if applicable, the date on which the program or activity will end, or*
>
> *(b) an order of the minister responsible for this Act that*
>
> *(i) states that a program or activity, which provides one or more services through one ministry working on behalf of one or more other public bodies or agencies, is a common or integrated program or activity, and*
>
> *(ii) includes, with respect to the program or activity, the information set out in paragraph (a) (ii).*

Saskatchewan's *Freedom of Information and Protection of Privacy Act Regulations* also require an Information Sharing Agreement for "common or integrated services".

> *17.1 (1)(b) "information sharing agreement" means an agreement that governs the collection, use and disclosure of personal information by the parties involved in the provision of a common or integrated service and that meets the requirements of subsection (2).*
>
> *(2) An information sharing agreement must contain the following:*
>
> *(a) a description of the common or integrated service to be provided;*
>
> *(b) a description of the purposes or expected outcomes of the common or integrated service;*

(c) provisions setting out the obligations of a party respecting the security and safeguarding of personal information received by that party;

(d) provisions that prohibit the subsequent use and disclosure of the personal information for purposes not related to the common or integrated service except:

(i) with the consent of the person to whom the information relates; or

(ii) if required or authorized by law;

(e) provisions for the withdrawal of a party and, in the case of a withdrawal, provisions that:

(i) prohibit any further use or disclosure of the personal information received by that party except:

(A) with the consent of the person to whom the information relates; or

(B) if required or authorized by law; and

(ii) specify the ongoing obligations of that party to secure and safeguard the personal information;

(f) provisions for the termination of the information sharing agreement and, in the case of a termination, provisions that:

(i) prohibit any further use or disclosure of the personal information received by the parties except:

(A) with the consent of the person to whom the information relates; or

(B) if required or authorized by law; and

(ii) specify the ongoing obligations of the parties to secure and safeguard the personal information;

(g) any other provisions that the minister considers necessary.

(3) For the purposes of clause 29(2)(u) of the Act, personal information may be disclosed to a party to an information sharing agreement entered into for the purposes of providing a common or integrated service:

(a) if that information is disclosed in accordance with the agreement for any or all of the following purposes:

(i) determining the eligibility of an individual to receive the common or integrated service;

(ii) assessing and planning the common or integrated service and delivering that service to an individual or that individual's family; or

(b) if consent to the disclosure was obtained pursuant to any other Act or regulation that does not require the consent to be in writing.

(4) If the Royal Canadian Mounted Police participates in providing a common or integrated service, the requirements of subsection (3) are met if the Royal Canadian Mounted Police enters into a single arrangement in writing with a government institution that is involved in the provision of the common or integrated service, under which the Royal Canadian Mounted Police signifies that it will comply with the terms governing the collection, use and disclosure of personal information contained in the information sharing agreement applicable to the common or integrated service in which the Royal Canadian Mounted Police participates.

(5) Notwithstanding section 18, consent to the use and disclosure of personal information for the purposes of receiving a common or integrated service is not required to be in writing if:

> *(a) the individual providing consent is informed of the anticipated uses and disclosures of the individual's personal information; and*
>
> *(b) the person who obtained the consent records the following information and signs the record:*
>
> > *(i) the date on which consent was obtained;*
> >
> > *(ii) the manner by which consent was obtained, whether the consent was obtained in person, by way of telephone or otherwise;*
> >
> > *(iii) the anticipated uses and disclosures of personal information the individual consented to;*
> >
> > *(iv) any restrictions on the consent that was provided.*

Section 46.2 of *New Brunswick's Right to Information and Protection of Privacy Act* also requires agreements for common or integrated services, programs, or activities of public bodies:

46.2(1) Each public body that provides a common or integrated service, program or activity shall enter into a written agreement with the other public bodies and nonpublic bodies that are also providing that common or integrated service, program or activity.

46.2(2) A written agreement entered into under subsection (1) shall

> *(a) provide for the protection of the personal information disclosed for the purpose of the common or integrated service, program or activity against risks, including unauthorized access, use, disclosure or disposal and provide for the secure disposal of the information, and*
>
> *(b) contain the information prescribed by regulation.*

46.2(3) A non-public body that enters into a written agreement under subsection (1) shall comply with

> *(a) the duties imposed on the non-public body under the agreement, and*
>
> *(b) the same requirements concerning the protection, retention and secure disposal of personal information that the public body is required to comply with under this Act and the regulations.*

Appendix F – 2020 Global Privacy Assembly Resolution on Artificial Intelligence

The 2020 GLOBAL PRIVACY ASSEMBLY therefore resolves to:

1. Urge organisations that develop or use AI systems to consider implementing the following accountability measures:

(1)Assess the potential impact to human rights (including data protection and privacy rights) before the development and/or use of AI;

(2)Test the robustness, reliability, accuracy and data security of AI before putting it into use, including identifying and addressing bias in the systems and the data they use that may lead to unfair outcomes;

(3)Keep records of impact assessment, design, development, testing and use of AI;

(4)Disclose the results of the data protection, privacy and human rights impact assessment of AI;

(5)Ensure transparency and openness by disclosing the use of AI, the data being used and the logic involved in the AI;

(6)Ensure an accountable human actor is identified (a) with whom concerns related to automated decisions can be raised and rights can be exercised, and (b) who can trigger evaluation of the decision process and human intervention;

(7)Provide explanations in clear and understandable language for the automated decisions made by AI upon request;

(8)Make human intervention on the automated decision made by AI upon request;

(9)Continuously monitor and evaluate the performance and impacts of AI by human beings, and act promptly and firmly to address identified issues;

(10)Implement whistleblowing / reporting mechanisms about non-compliance or significant risk in the use of AI;

(11)Ensure the auditability of AI systems and be prepared to demonstrate accountability to data protection authorities on request; and

(12)Engage in multi-stakeholder discussions (including with non-governmental organisations, public authorities and academia) to identify and address the wider socio-economic impact of AI and to ensure algorithmic vigilance.

2. Urge organisations that develop or use AI systems to implement accountability measures which are appropriate regarding the risks of interference with human rights.

3. Call upon all members of the Global Privacy Assembly to work with organisations that develop or use AI systems in their jurisdictions and globally to promote the principles adopted in its 2018 resolution, and accountability in the development and use of AI, and the adoption of accountability measures;

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

5. Encourage governments, public authorities, standardisation bodies, organisations developing or using AI systems and all other relevant stakeholders to work with data protection authorities in establishing principles, standards, and accountability mechanisms, such as certification, for the purpose of demonstrating legal compliance, accountability and ethics in the development and use of AI systems.

Appendix G – References to Indigenous governments and organizations in Canadian Access and Privacy Statutes

British Columbia

Schedule 1 of British Columbia's *Freedom of Information and Protection of Privacy Act* provides definitions:

> *"aboriginal government" means an aboriginal organization exercising governmental functions;*

Section 16 of that statute includes references to Aboriginal governments:

> *Disclosure harmful to intergovernmental relations or negotiations*
>
> *16 (1)The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to*
>
> > *(a)harm the conduct by the government of British Columbia of relations between that government and any of the following or their agencies:*
> >
> > > *(i)the government of Canada or a province of Canada;*
> > >
> > > *(ii)the council of a municipality or the board of a regional district;*
> > >
> > > *(iii)an aboriginal government;*
> > >
> > > *(iv)the government of a foreign state;*
> > >
> > > *(v)an international organization of states,*
> >
> > *(b)reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies, or*
> >
> > *(c)harm the conduct of negotiations relating to aboriginal self government or treaties.*

Section 22 references potential harms to Aboriginal claims, disputes or grievances

> *Disclosure harmful to personal privacy*
>
> *22 (1)The head of a public body must refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.*
>
> *(2) In determining under subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether*
>
> > *[…]*

(d)the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

Alberta

Alberta's *Freedom of Information and Protection of Privacy Act* has references in similar sections as the BC statute, though has an additional reference that provides authority for public bodies to collect information indirectly for the purposes of researching or validating claims or grievances of Aboriginal people:

Section 1 - Definitions

(i) "local government body" means … (viii) a Metis settlement established under the Metis Settlements Act, (ix) the Metis Settlements General Council established under the Metis Settlements Act,…

Disclosure harmful to personal privacy

17 (5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether (d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

Disclosure harmful to intergovernmental relations

21(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm relations between the Government of Alberta or its agencies and any of the following or their agencies:

(i) the Government of Canada or a province or territory of Canada, (ii) a local government body,

(iii) an aboriginal organization that exercises government functions, including

(A) the council of a band as defined in the Indian Act (Canada), and

(B) an organization established to negotiate or implement, on behalf of aboriginal people, a treaty or land claim agreement with the Government of Canada,

Manner of collection of information

34(1) A public body must collect personal information directly from the individual the information is about unless …

(o) the information is collected for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people.

Federal

The Federal *Access to information Act* also has the most detailed definition and identification of Aboriginal governments. It would appear that this list would likely tie in directly with the application of section 13(e) of that Act.

> *Information obtained in confidence*
>
> *13 (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Part that contains information that was obtained in confidence from*
>
> > *(a) the government of a foreign state or an institution thereof;*
> >
> > *(b) an international organization of states or an institution thereof;*
> >
> > *(c) the government of a province or an institution thereof;*
> >
> > *(d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government; or*
> >
> > *(e) an aboriginal government.*
>
> *[…]*
>
> *Definition of aboriginal government*
>
> *(3) The expression aboriginal government in paragraph (1)(e) means*
>
> > *(a) Nisga'a Government, as defined in the Nisga'a Final Agreement given effect by the Nisga'a Final Agreement Act;*
> >
> > *(b) the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the Westbank First Nation Self-Government Act;*
> >
> > *(c) the Tlicho Government, as defined in section 2 of the Tlicho Land Claims and Self-Government Act;*
> >
> > *(d) the Nunatsiavut Government, as defined in section 2 of the Labrador Inuit Land Claims Agreement Act;*
> >
> > *(e) the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act;*
> >
> > *(e.1) the Tla'amin Government, as defined in subsection 2(2) of the Tla'amin Final Agreement Act;*
> >
> > *(f) the Tsawwassen Government, as defined in subsection 2(2) of the Tsawwassen First Nation Final Agreement Act;*
> >
> > *(f.1) the Cree Nation Government, as defined in subsection 2(1) of the Cree Nation of Eeyou Istchee Governance Agreement Act or a Cree First Nation, as defined in subsection 2(2) of that Act;*
> >
> > *(g) a Maanulth Government, within the meaning of subsection 2(2) of the Maanulth First Nations Final Agreement Act;*

(h) Sioux Valley Dakota Oyate Government, within the meaning of subsection 2(2) of the Sioux Valley Dakota Nation Governance Act; or

(i) the council of a participating First Nation, as defined in section 2 of the Anishinabek Nation Education Agreement Act.

The remaining Acts listed below contain reference to Aboriginal governments to varying extents, under intergovernmental affairs, unreasonable invasion of personal privacy, or manner of collection sections.

Nova Scotia

Freedom of Information and Protection of Privacy Act

Intergovernmental affairs

12 (1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm the conduct by the Government of Nova Scotia of relations between the Government and any of the following or their agencies:

(i) the Government of Canada or a province of Canada,

(ii) a municipal unit or the Conseil scolaire acadien provincial,

(iii) an aboriginal government,

(iv) the government of a foreign state, or

(v) an international organization of states;…

Personal information

20 (1) The head of a public body shall refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's personal privacy.

(2) In determining pursuant to subsection (1) or (3) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Nova Scotia or a public body to public scrutiny;

(b) the disclosure is likely to promote public health and safety or to promote the protection of the environment;

(c) the personal information is relevant to a fair determination of the applicant's rights;

(d) the disclosure will assist in researching the claims, disputes or grievances of aboriginal people;

Prince Edward Island

Freedom of Information and Protection of Privacy Act

Disclosure harmful to personal privacy

15(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether …

> *d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;*

Manner of collection of information

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

> *(k) the information is collected for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people….*

Ontario

Freedom of Information and Protection of Privacy Act

Relations with Aboriginal communities

15.1 (1) A head may refuse to disclose a record where the disclosure could reasonably be expected to,

> *(a) prejudice the conduct of relations between an Aboriginal community and the Government of Ontario or an institution; or*
>
> *(b) reveal information received in confidence from an Aboriginal community by an institution.*

(2) In this section,

"Aboriginal community" means,

> *(a) a band within the meaning of the Indian Act (Canada),*
>
> *(b) an Aboriginal organization or community that is negotiating or has negotiated with the Government of Canada or the Government of Ontario on matters relating to,*
>
> > *(i) Aboriginal or treaty rights under section 35 of the Constitution Act, 1982, or*
> >
> > *(ii) a treaty, land claim or self-government agreement, and*
>
> *(c) any other Aboriginal organization or community prescribed by the regulations.*

60 (1) The Lieutenant Governor in Council may make regulations,

(0.a.1) prescribing Aboriginal organizations and communities for the purposes of clause (c) of the definition of "Aboriginal community" in subsection 15.1 (2);

Yukon

Access to Information and Protection of Privacy Act

Disclosure harmful to intergovernmental relations or negotiations

20(1) A public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to

(a) harm the conduct by the Government of the Yukon of relations between that Government and any of the following or their agencies

(i) the Government of Canada or a province or territory of Canada,

(ii) the council of a municipality,

(iii) a Yukon First Nation government or similar government established under a land claims settlement, the governing body of a band under the Indian Act (Canada), or other aboriginal authority or organization,

(iv) the government of a foreign state, or

(v) an international organization of states;

(b) reveal information received in confidence from a government, council or organization listed in paragraph (a) or their agencies; or

(c) harm the conduct of negotiations relating to or arising from aboriginal self government or land claims settlements.

(3) Subsection (1) does not apply to information in a record that has been in existence for 15 or more years other than information in a record in respect of unfinished negotiations relating to aboriginal self-government or land claims settlements.

Northwest Territories

Access to Information and Protection of Privacy Act

Disclosure prejudicial to intergovernmental relations

16. (1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to

(a) impair relations between the Government of the Northwest Territories and any of the following or their agencies:

(i) the Government of Canada or the government of a province or territory,

(ii) an aboriginal organization exercising governmental functions, including, but not limited to (A) a band council, and (B) an organization established to

negotiate or implement, on behalf of aboriginal people, a treaty or land claim agreement or treaty with the Government of Canada,

(iii) a municipal council or other local authority,

(iv) the government of a foreign state,

(v) an international organization of states;

(b) prejudice the conduct of negotiations relating to aboriginal self-government or to a treaty or land claims agreement; or

(c) reveal information received, explicitly or implicitly, in confidence from a government, local authority or organization referred to in paragraph (a) or its agency.

Disclosure harmful to conservation

19. The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to result in damage to or interfere with the conservation of (a) fossil sites or natural sites; (b) sites having an anthropological or heritage value or aboriginal cultural significance; or (c) any rare, endangered, threatened or vulnerable form of life.

Personal privacy of third party

23(3) In determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the

Government of the Northwest Territories or a public body to public scrutiny;

(b) the disclosure is likely to promote public health and safety or to promote the protection of the environment;

(c) the personal information is relevant to a fair determination of the applicant's rights;

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;

Nunavut

Access to Information and Protection of Privacy Act

Disclosure prejudicial to intergovernmental relations

16. (1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to

(a) impair relations between the Government of Nunavut and any of the following or their agencies:

(i) the Government of Canada or a province or territory,

(ii) an aboriginal organization exercising governmental functions, including, but not limited to (A) a band council, and (B) an organization established to negotiate or implement, on behalf of aboriginal people, a treaty or land claim agreement or treaty with the Government of Canada,

(iii) a municipal or settlement council or other local authority,

(iv) the government of a foreign state,

(v) an international organization of states;

(b) prejudice the conduct of negotiations relating to aboriginal self-government or to a treaty or land claims agreement; or

(c) reveal information received, explicitly or implicitly, in confidence from a government, local authority or organization referred to in paragraph (a) or its agency.

Disclosure harmful to the conservation of heritage sites

19. The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to result in damage to or interfere with the conservation of

(a) fossil sites or natural sites;

(b) sites having an anthropological or heritage value or aboriginal cultural significance; or

(c) any rare, endangered, threatened or vulnerable form of life.

Personal privacy of third party

23 (3) In determining whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including …(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;