

October 9, 2026

Ms. Keri-Lynn Power
Committee Chair
Access to Information and Protection of Privacy Act Statutory Review 2025
2nd Floor, Beothuck Building
20 Crosbie Place
St. John's, NL
A1B 3Y8

Via Email: ATIPPAReview@gov.nl.ca

Dear Committee Chair Power,

Thank you for your letter of July 17, 2026, consulting Memorial University regarding the statutory review of the *Access to Information and Protection of Privacy Act, 2025*.

I am pleased to submit herewith for your consideration Memorial University's submission.

Please do not hesitate to contact me or Ms. Maggie Noseworthy, University Privacy Officer, should you desire further information or clarification. We are pleased to be involved with such important work.

Sincerely,



Janet Morrison, PhD
President and Vice-Chancellor

Enclosure: Memorial University ATIPPA Review Submission

c: Mr. Scott Worsfold, General Counsel
Ms. Maggie Noseworthy, University Privacy Officer

Ref: O/JM/POWER1009 (2026)



Memorial University
Submission to
ATIPPA Statutory Review Committee 2025
on the Review of the
Access to Information and Protection of Privacy Act, 2015

9 October 2026

Table of Contents

EXECUTIVE SUMMARY	3
I. INTRODUCTION	6
II. APPLICATION TO HIGHER EDUCATION	6
III. RECOMMENDATIONS.....	9
Recommendation 1: Definition of Personal Information	9
Recommendation 2: Exception to Access – s. 22 Published Material	13
Recommendation 3: Exception to Access – s. 30 Legal Advice.....	14
Recommendation 4: Exception to Access – s. 33 Workplace Investigation	16
Recommendation 5: Limit on Concurrent Access Requests from the Same Applicant	18
Recommendation 6: Fee Considerations.....	19
Recommendation 7: Record(s) already possessed by an Applicant	22
Recommendation 8: Preventing Abuse of the ATIPPA, 2015 – s. 21 Disregarding a Request.....	23
Recommendation 9: Duty to Assist.....	31
Recommendation 10: Protection for IT Security Arrangements	33
Recommendation 11: Access to Electronic Records (s. 11 and 20)	35
Recommendation 12: Privacy Impact Assessments (s. 72).....	38
Recommendation 13: Common or Integrated Programs	39
IV. GAPS IN THE LEGISLATION/OVERSIGHT CONCERNS	42
Recommendation 14: A Deadline for Complying with the Commissioner’s Recommendation(s).....	43
Recommendation 15: Application of the Rules of the Supreme Court, 1986 & the Appeal Process.....	44
APPENDICES.....	47
Appendix A: Volume of ATIPP requests and OIPC complaint investigations since 2016.....	47

EXECUTIVE SUMMARY

Summary of Recommendations

1. Memorial University recommends that the definition of Personal Information in the *ATIPPA, 2015* be amended to protect, as personal information of the author, “correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature and replies to that correspondence that would reveal the contents of the original correspondence.”

Memorial University further recommends an amendment in the definition of Personal Information to clarify that the individual’s personal views or opinions about another person that are provided in relation to workplace conduct are not the personal information of the person complained about except where relevant to a workplace investigation.

2. Memorial University recommends a revision of s. 22 to allow a public body additional time to review, analyze, de-identify and report on administrative research prior to releasing it in response to an ATIPP request, particularly when this research involves individual identifiable raw data responses.
3. Memorial University recommends a revision or clarification to s. 100 of the legislation that reflects the current state of the law in this province regarding solicitor-client, and litigation privileged records, and production of these records to the commissioner (2023 NLCA 27, 2022 NLSC 70). Specifically, the university recommends the addition of explicit language that states that the commissioner may not compel production of solicitor-client and/or litigation privileged records; and further, that a public body has discharged its burden by complying with the civil procedure standard of identifying privileged documents, asserting a claim for privilege, and noting the type of privilege applied.
4. Memorial University recommends that an amendment to section 33 provide that records pertaining to a workplace investigation be withheld until *after the investigator’s report has been issued*.
5. Memorial University recommends a limit on the number of concurrent requests made by the same applicant.
6. Memorial University recommends:
 - the restoration of an application fee
 - amendment of s. 25(3) to permit charges for certain types of activities
 - clarification in s.26 that the Commissioner’s decision under s. 26 is final and cannot be the subject of a further Complaint to the Commissioner or appeal to Court under s. 55.
7. Memorial University recommends that the *ATIPPA, 2015* should be amended to permit a public body to refuse to provide records where there is evidence that the applicant already has them in their possession.
8. Memorial University recommends that section 21 be amended to provide better oversight of abuses of the legislation and to give remedial effect to that purpose.
9. Memorial University recommends clarification on the review process and enforcement in respect of the duty to assist, taking into consideration:

- the cost of compliance
 - timely access
 - the need for finality of the process
10. Based on the position and best practices of security professionals across the country, Memorial University recommends stronger, more inclusive language in the ATIPPA to provide for the protection from disclosure of information respecting IT systems. This would be accomplished by having a separate section in the ATIPPA dedicated to IT security protection.
 11. Memorial University asserts that the *ATIPPA, 2015* does not and should not afford a right of access to records in native format and recommends that no change be made to the legislation in that regard.
 12. Memorial University recommends that section 72 be amended by adding a subsection as follows:
 - (5) Notwithstanding section 72(1) and (2), Memorial University shall, during the development of a program or service by Memorial University, submit to the Head:
 - (a) A privacy impact assessment for the Head'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
 13. Memorial University recommends that s.72 be amended by adding subsections as follows:
 - (6) Notwithstanding section 72(3) and (4), Memorial University shall notify the commissioner of a common or integrated program or service in connection with administrative matters, but not academic programming matters, at an early stage of developing the program or service.
 - (7) Notwithstanding section 72(3) and (4), the Head of Memorial University shall, where the Head receives a privacy impact assessment respecting a program or service described in subsection 6 for which disclosure of personal information may be permitted under paragraph 68 (1)(u), the Head shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.

Gaps in the Legislation/Oversight Concerns

14. Memorial University recommends to:
 - Amend the legislation to clearly delineate that there is a statutory deadline for compliance with the Commissioner's recommendations
 - Extend the number of business days that a public body has to comply with the Commissioner's recommendation to at least 20 business days.
15. Memorial recommends:
 - That the legislation be amended to clarify that a de novo hearing shall proceed as an expedited hearing on the basis of affidavit evidence subject to further application to the Court for additional steps under Rule 17A.09.
 - That the first appearance date shall proceed as a case management meeting at which the parties are to discuss any applications contemplated under Rule 17A.09 and

scheduling deadlines.

- That further recourse to the *Rules of the Supreme Court, 1986* be prohibited absent an order of the Court under Rule 17A.09 (as contemplated by the application provision of the *Rules of the Supreme Court, 1986* in Rule 1.02).
- That all *ATIPPA, 2015* appeals be case managed, with the first date serving as the first case management meeting.
- That a public body be required to file an audit copy of the records under seal with the Court without the necessity of a sealing application.

I. INTRODUCTION

As Newfoundland and Labrador's only university, Memorial has a special obligation to the people of this province. Established as a memorial to the Newfoundlanders who lost their lives in active service during the First and Second World Wars, Memorial University draws inspiration from these shattering sacrifices of the past as we help to build a better future for our province, our country and our world.

We are a multi-campus, multi-disciplinary, public, teaching/research university committed to excellence in everything we do. We strive to have national and global impact, while fulfilling our social mandate to provide access to university education for the people of the province and to contribute to the social, cultural, scientific and economic development of Newfoundland and Labrador and beyond.

Memorial has more than 16,721 students who can avail of numerous program options spread across 5 campuses and more than 90,000 alumni active throughout the world. From local endeavors to research projects of international scope, Memorial's impact is felt far and wide. As one of the top 20 research universities in Canada, Memorial has more than 30 research centres and received more than \$170 million in research funding in 2023.

The public rightly requires transparency and accountability of Memorial University. Memorial recognizes its role as a public institution and its important obligation to govern itself in the public trust.

Following proclamation of the *Access to Information and Protection of Privacy Act (ATIPPA)* in 2005, the university established an Information Access and Privacy ("IAP") Office, led by the University Privacy Officer. Its mandate is to develop and implement policy, procedures and best practices in information access and privacy protection; to conduct privacy impact assessments of projects and programs to identify privacy risks and recommend measures to mitigate those risks; to provide strategic and day-to-day advice to the university on all matters pertaining to access and privacy; to manage ATIPP requests, and; to deliver access and privacy training to the university community.

The university's Privacy policy was established in 2008, updated in 2026 and its guiding principle states:

Memorial University is entrusted with the personal information of its students, employees, alumni, donors, research participants, retirees and others and is committed to excellence in its management of this information.

II. APPLICATION TO HIGHER EDUCATION

We note the university is not an agency of the provincial government and that it has autonomy from the government in order to fulfil its mandate. In accordance with the *Memorial University Act*, university governance is bicameral and divided between the Board of Regents and the Senate. The Board of Regents has responsibility for management, administration and control of the property, revenue, business and affairs of the university and the Senate has responsibility for academic matters. This

division of responsibilities is very common in universities. In respect of the administrative activities at Memorial University, Memorial is much the same as any public body administering the *ATIPPA, 2015*. In respect of academic matters, however, the *ATIPPA, 2015*'s application to a higher education body presents challenges.

The legislation does not effectively account for the principles of autonomy, academic freedom and collegial decision-making that are embedded in the institution. The *ATIPPA, 2015* is designed primarily for government bodies where employees' work is deemed to be directed by the public body's leadership. However, a great deal of work undertaken in academic and research activity is not directed by the university's executive. For example, research is curiosity driven and conceived of and carried out by individual researchers, much of it as studies. Similarly, while the university's Senate approves courses, instructors determine how best to deliver their teaching. As well, much work carried out by instructors is outside professional work that is not directed by the university executive.

Academic freedom is a fundamental principle and privilege of academics. Fully described in Article 2 of Memorial's collective agreement with the Memorial University of Newfoundland Faculty Association, two points merit highlighting:

2.03 Therefore, the Parties agree to uphold the right of ASMs to teach, to learn, to carry out research, to publish, to comment, to criticize, to acquire and disseminate knowledge, to create, and to perform; all of these without deference to prescribed doctrine.

2.04 Academic freedom includes the right to discuss and criticize policies and actions of the University and the Association and protects against the imposition of any penalty by either Party for exercising that right.

We highlight the above to draw your attention to the distinction between personal information and 'work product.' Many courts and tribunals have considered this distinction. Although not a defined term in the *ATIPPA, 2015*, work product is covered in two provisions in the *ATIPPA* that illustrate its intended application to environments that presume its employees are acting as its agents and not independently of the employer:

- 40(2)(f)

This provision states that disclosure of information about an employee's position, functions and salary range is not an unreasonable invasion of the employee's privacy. The "position" and "functions" aspects of this provision are equated to "work product." It concerns the extent to which records produced by or about an employee relate to the employee's "functions" and are not, therefore, the employee's personal information.

- 40(2)(h)

This provision states that disclosure of an opinion of an employee or other third party given in the course of performing services for a public body is not an unreasonable invasion of the employee's privacy. This provision assumes that opinions produced by employees of a public body in the course

of performing services for their employer are not their personal information and are, instead, part of their “work product.”

The *ATIPPA, 2015* effectively assigns accountability for actions of its employees to the public body. At Memorial University, however, the governance structure and collegial decision-making in academic matters (including academic policy, academic program reviews, peer review, course offerings, and pedagogy) mean that many decisions pertaining to academic matters are not directed by the university’s president (the public body head under the *ATIPPA, 2015*) nor by administrators. For example, academic program regulations are governed by the Senate. In addition to regulating the conduct of its meetings and determining degrees awarded and to whom, the Senate’s powers under the *Memorial University Act* include:

- determine the conditions of matriculation and entrance, the standing to be allowed students entering the university and all related matters;
- receive, consider and determine proposals or recommendations of a faculty council or other body as to courses of study and all related matters;
- regulate instruction and to determine the methods and limits of instruction;
- determine the conditions on which candidates shall be received for examination, to appoint examiners and to determine the conduct of all examinations;
- prepare the calendar of the university for publication;
- appoint committees that it considers necessary and to confer upon the committees power and authority act for the senate in and in relation to matters which the Senate considers expedient and to appoint other committees that the Senate considers expedient to act in an advisory capacity; and,
- exercise disciplinary jurisdiction with respect to students in attendance at the university, by way of appeal from a decision of the faculty council.

University governance can be described as collaborative governance in which power is shared and balanced between governing bodies. It is a unique form of accountability derived from the tenets of autonomy, independence, academic freedom and governing in the public trust.

Collegial decision-making is the basis of decision-making about academic matters and cannot function without faculty participation.

Similarly, in accordance with long-standing practice, many of the records generated by faculty in the course of conducting research, developing teaching materials and creating knowledge through publication and presentation are not in the custody and control of the university.

In a 2011 report from the Information and Privacy Commissioner of Ontario concerning a university’s custody and control of records held by members of the university’s faculty association (APUO), the Commissioner noted:

The significant conclusions I have reached in this regard are:

1. *records or portions of records in the possession of an APUO member that relate to personal matters or activities that are wholly unrelated to the university's mandate, are not in the university's custody or control;*
2. *records relating to teaching or research are likely to be impacted by academic freedom, and would only be in the university's custody and/or control if they would be accessible to it by custom or practice, taking academic freedom into account;*
3. *administrative records are prima facie in the university's custody and control, but would not be if they are unavailable to the university by custom or practice, taking academic freedom into account.*

Final Order PO-3009-F of the Information and Privacy Commissioner, Ontario

Available at: <https://norma.lexum.com/ipc-cipvp/orders/en/133734/1/document.do>

To summarize, administration of the *ATIPPA, 2015* at Memorial University contends with complexities that derive from its unique governance structure and, as well, the important principles of autonomy and academic freedom that, as concluded in the report by the Ontario commissioner in respect of an Ontario university, impact on Memorial's custody and control of records held by its academic staff members.

We, therefore, ask you to consider all of the above in light of the recommendations that follow. The first recommendation pertains to the definition of personal information; two recommendations relate to exceptions to disclosure; the next four pertain to process matters; and the final recommendation pertains to oversight. To provide context as you review our submission, Appendix A contains the volume of ATIPP requests, OIPC complaint investigations and ATIPP-related court cases received by the university since 2016.

III. RECOMMENDATIONS

Recommendation 1: Definition of Personal Information

Our Justification

Memorial University has experienced several ATIPP requests and OIPC access complaint investigations in which the definition of personal information dealing with opinions has been problematic. The definition states, in part:

"personal information" means recorded information about an identifiable individual, including
(viii) the opinions of a person about the individual, and
(ix) the individual's personal views or opinions, except where they are about someone else;

The Act provides significant protection for personal information. However, the definition excludes protection for some types of opinions and views that one might, as a principle of justice and fairness, expect to be protected. The definition of “personal information” includes the opinions of another person about the individual. Logically, of course, this part of the definition would, and does, apply to public employees’ personal views or opinions about another person in the course of employment. Say, for example, a public employee expresses an opinion about a person who is applying for a benefit. Clearly, this ought to be the personal information of the person applying for the benefit.

However, the principle is problematic when the person expressing the opinion is not doing so in their capacity as a public employee or is doing so in an inherently personal capacity, or in a context where discretion and confidentiality are expected. For example, consider the case of an employee who emails their supervisor or meets with their supervisor regarding questionable behaviour of another employee. The employee may simply be seeking advice or guidance, may not want to make a formal complaint, and may expect that the information they share about their co-worker will be kept confidential. However, under the current definition of “personal information,” the email or any meeting notes arising from that interaction may have to be disclosed to the employee with questionable behaviour if that person files a personal information request. Such disclosure could cause stress and humiliation to the employee who brought the issue forward, all because this “opinion” will be considered the applicant’s personal information and not the personal information of the person who provided it.

Memorial processed an ATIPP request in which one of the responsive records was an email in which Faculty Member A confidentially expressed personal feelings and views of herself that were tangentially connected to Faculty Member B, the ATIPP applicant. When the applicant filed a complaint with the OIPC, the OIPC took the position that the information was not the personal information of Faculty Member A but instead was Faculty Member B’s personal information. The OIPC recommended releasing this information to the applicant. Faculty Member A’s views were not afforded protection under s. 40 because they were not, pursuant to the OIPC’s interpretation, personal information of Faculty Member A.

These examples illustrate an inconsistency between the protection of personal information under the Act and its definition. The protection of personal information under the Act, represents a codification of the recognition that “information about a person ... is in a fundamental way his own, for him to communicate or retain for himself as he sees fit”.¹ The Supreme Court of Canada explained in *R v Dymnt* as follows:

Finally, there is privacy in relation to information. This too is based on the notion of the dignity and integrity of the individual. As the Task Force put it (p. 13): "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit." In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to

whom, and restricted to the purposes for which it is divulged, must be protected. Governments at all levels have in recent years recognized this and have devised rules and regulations to restrict the uses of information collected by them to those for which it was obtained; see, for example, the [Privacy Act](#), S.C. 1980-81-82-83, c. 111.

The protection is for a privacy interest which “connotes concepts of intimacy, identity, dignity and integrity of the individual.” However, in practice, what the above examples illustrate is that Employee A can express her intimate thoughts and fears to a supervisor, which thoughts and fears connote concepts of intimacy, dignity and her personal integrity, but because they arise in a context involving Employee B, they are – as the Commissioner sees it – not her personal information but Employee B’s. This is notwithstanding the fact that the information in question in no way relates to the dignity or integrity of Employee B. In other words, the privacy interest that is intended to be protected is in fact diminished, because of a problem with the definition of “personal information.”

The proviso that a person’s personal views or opinions about someone else’s are the other person’s personal information finds its footing in a 2007 report from the Information and Privacy Commissioner. At that time, the legislation indicated that personal information included the opinions of a person about the individual and the individual’s personal views or opinions. The result was that Person A’s personal opinion about Person B was the personal information of both Person A and Person B. At issue was a request by an individual for harassment complaints made about him. The Commissioner noted the ambiguity in the legislation and resolved it in favour of the individual complained about.

Leaving the definition of personal information as it currently stands has a chilling effect for those individuals who seek assistance in relation to workplace conduct, and who choose not to formalize a complaint. Based on its current application, the most intimate thoughts of a person who seeks guidance from, for instance, a sexual harassment advisor, will be subject to disclosure to the very individuals that the person fears. As a result, Memorial University asks that a policy decision be made, which recognizes that the privacy interest in such conversations belong to the individuals having them – not the persons who may be tangentially the subject.

The definition is also problematic insofar as it captures opinions or views of persons who are not public body employees or are provided to the university on an unsolicited basis.

In one ATIPP request to the university, an applicant made a personal information request for all records regarding himself and a third party. However, neither of these individuals was a public body employee and each had an expectation of privacy. Nevertheless, on investigating, the OIPC was of the opinion that the views expressed by the third party ought to be released to the applicant because they did not constitute the third party’s personal information. On this basis, the third party would not have a right of notice under s. 19, or opportunity to give consent, or any of the protections afforded under s. 40.

Similarly, unsolicited correspondence to the university containing personal views or opinions of a member of the public about a university member merits, at a minimum, consideration under s. 19 (third

party notice) and under s. 40 (protection of personal information). However, based on the definition of Personal Information, the unsolicited opinion would belong to the person the opinion is about. The member of the public, while having an expectation of privacy, would be entitled to none.

The current definition of personal information presents further challenges when considered in the context of the university's Protected Disclosure Policy. The goal of this policy is to enable and encourage members of the university community to report incidents of wrongdoing, under the auspices that such reporting will be treated confidentially without risk of retaliation against the reporting party. The societal necessity and importance of such a reporting mechanism is acknowledged by the legislature as per the *Public Interest Disclosure and Whistleblower Protection Act* or "*PIDA*", which serves to protect public employees who disclose acts of wrongdoing in the workplace.

Memorial University was specifically excluded from this legislation, as noted by the Office of the Citizen's Representative in their annual report of 2022-2023, because Memorial has its own internal policy structure that addresses protected disclosures; as such, it stands to reason that members of the university community who invoke the protected disclosure policy would be afforded the same protections offered to public employees under *PIDA*. However, the *ATIPPA, 2015* presents an unfortunate loophole to the functionality of the university's protected disclosure process, in that an ATIPP applicant may make a request for personal information that involves records created under the protected disclosure policy, that may identify individuals who have invoked the policy. Based on the current definition of personal information, an ATIPP applicant could potentially receive details of a protected disclosure complaint made against them, thus thwarting the very intention of this reporting mechanism. This loophole then undermines any investigatory process or findings that result and has a chilling effect on the protected disclosure process.

The impact of this loophole is apparent in a report from this province's *Office of the Information and Privacy Commissioner* (Report A.2025.O40), in which the Commissioner determined that records pertaining to protected disclosures at Memorial are not protected from disclosure in response to an ATIPP request. The omission of a specific exemption for these records, combined with the current definition of personal information, has had a chilling effect upon protected disclosures at Memorial. In fact, following the issuance of the OIPC's report on the matter, Memorial was advised by those who had made the protected disclosures that they would never do so again. This is an oversight that needs to be rectified.

Paragraph (ix) in the definition of personal information does not restrict itself to public employees' opinions. It applies to opinions of any person, regardless of context, and even unsolicited opinions. Ontario's *Freedom of Information and Protection of Privacy Act* deals with this conundrum by adding the following to its definition of personal information:

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence

Recommendation #1

Memorial University recommends that the definition of Personal Information in the *ATIPPA, 2015* be amended to protect, as personal information of the author, “correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence.”

Memorial University further recommends an amendment in the definition of Personal Information to clarify that the individual’s personal views or opinions about another person that are provided in relation to workplace conduct are not the personal information of the person complained about except where relevant to a workplace investigation.

Recommendation 2: Exception to Access – s. 22 Published Material

Our Justification

Increasingly, the university receives ATIPP requests for raw administration survey data and administrative survey individual responses, often referred to as “administrative research”. Although these may appear to be reasonable general access requests for information, and are distinguishable from a record that contains “research information” as enumerated in s. 5 (1)(g) of the *ATIPPA, 2015*, they are often wrought with considerable privacy risks to third party personal information. For example, an administrative survey that is distributed to the university community (which may include students, staff, faculty, or any combination of these groups) may result in raw data responses that contain personal information, even if a survey cautions against identifying oneself in an open-ended survey response field. In some cases, data responses to survey questions contain total author identification; other times the survey and/or the survey demographic itself may lend itself to identifiability.

For many of these ATIPP requests, the relevant department or unit that administered the survey is barely given time to collect the survey responses prior to providing them to our office to respond to an applicant’s request. In several instances, particularly when the survey audience includes the broader university community, these requests are submitted the day after a survey has closed, notice of which is generally explicitly communicated to the university community. In such cases, the relevant office or unit does not have an opportunity to process or assess the raw data, whether for use in a final report or some other form of release. In some cases, it may be the intention of an office or unit to share the results with a smaller audience or not to publish the results at all.

Arguably, the ability of an ATIPP applicant to request this data prior to its intended analysis removes the goal and function of a final report or memo when the data was collected for such a purpose. This also adds undue pressure to the offices collecting the information as they are now forced to either speed up their review or simply hand over all raw data to the IAP Office in order that they meet the legislative deadlines of responding to an ATIPP request.

Additionally, it is worth noting that the potential release of raw data information prior to its relevant assessment can be seen as a deterrent to those participating in the process to reveal full or frank responses or feedback. Arguably, this stands in opposition to the goal of such surveys, particularly when they are intended to impact upon and encourage institutional change.

On occasion, we have been able to respond to an ATIPP request while relying on s. 22(1)(b), to refuse to disclose a record that will be published or released within 30 business days after the applicant's request is received; but that is not always the case. It would, however, be helpful, in those cases where the university does intend to publish the collected data, in whichever format, if additional time were permitted under s. 22(1)(b), to allow for proper analysis and deidentification of raw data. We feel an additional 60 business days would be in the best interest of both the public body and the ATIPP applicant.

Memorial University recommends a revision to s. 22(1)(b), that states a public body may refuse to disclose a record or part of a record that is to be published or released to the public *within 90 business days* after the applicant's request is received.

Recommendation #2

Memorial University recommends a revision of s. 22 to allow a public body to refuse to disclose a record or part of a record, where that record is to be published or released within 90 business days. This will allow the public body appropriate time to review, analyze, de-identify and report on administrative research prior to releasing it in response to an ATIPP request, particularly when this research involves individual identifiable raw data responses.

[Recommendation 3: Exception to Access – s. 30 Legal Advice](#)

Our Justification

In *Newfoundland and Labrador (Justice and Public Safety) v. Newfoundland and Labrador (Information and Privacy Commissioner)*, 2022 NLSC 59 (JPS), the Supreme Court of Newfoundland and Labrador confirmed that the Commissioner does not have the authority to compel production of records over which a public body asserts solicitor-client privilege based on the language in the *ATIPPA, 2015*, and that privilege was appropriately invoked using the civil litigation standard. This precedent was later affirmed in a similar case, 2025 NLSC 70.

Two earlier Court decisions from other jurisdictions also support the Supreme Court of Newfoundland and Labrador's decision on this matter. Specifically, two decisions are notable: *Information and Privacy Commissioner v. University of Calgary*, 2016 SCC 53, and *Lizotte v Aviva Insurance Company of Canada*, 2016 SCC 52.

In the *University of Calgary* case, the Supreme Court of Canada imposed limitations on the powers of the Alberta Information and Privacy Commissioner to review solicitor-client privileged records. In that case,

s. 56(3) of the legislation provided that the Commissioner could compel production of records despite “any privilege of the law of evidence.” The Supreme Court of Canada ruled that solicitor-client privilege is not a “privilege under the law of evidence”, but rather a substantive, stand-alone privilege. The court stated:

The expression “any privilege of the law of evidence” does not require a public body to produce to the Commissioner documents over which solicitor-client privilege is claimed. Solicitor-client privilege is no longer merely a privilege of the law of evidence, but a substantive right that is fundamental to the proper functioning of our legal system. The disclosure of documents pursuant to a statutorily established access to information regime, separate from a judicial proceeding, engages solicitor-client privilege in its substantive, rather than evidentiary, context. To give effect to solicitor-client privilege as a fundamental policy of the law, legislative language purporting to abrogate it, set it aside or infringe it must be interpreted restrictively and must demonstrate a clear and unambiguous legislative intent to do so. Section 56(3) does not meet this standard and therefore fails to evince clear and unambiguous legislative intent to set aside solicitor-client privilege. This interpretive approach is not a renunciation of the modern approach to statutory interpretation, but recognizes legislative respect for fundamental values.

A similar result was reached by the Supreme Court of Canada with respect to litigation privilege in *Lizotte*. At issue in that case was whether an insurance Syndic could compel production of records under the *Act Respecting the Distribution of Financial Products and Services*. The Supreme Court concluded that it could not. While the Court did not describe litigation privilege as a “substantive right” like solicitor-client privilege, it nonetheless touched on its elevated status and indicated that the same requirements are needed to abrogate litigation privilege as are needed to abrogate solicitor-client privilege. The Court stated:

[64] There is of course no question that litigation privilege does not have the same status as solicitor-client privilege and that the former is less absolute than the latter. It is also clear that these two privileges, even though they may sometimes apply to the same documents, are conceptually distinct. Nonetheless, like solicitor-client privilege, litigation privilege is “fundamental to the proper functioning of our legal system” (Blood Tribe, at para. 9). It is central to the adversarial system that Quebec shares with the other provinces. As a number of courts have already pointed out, the Canadian justice system promotes the search for truth by allowing the parties to put their best cases before the court, thereby enabling the court to reach a decision with the best information possible: Penetanguishene Mental Health Centre v. Ontario, 2010 ONCA 197, 260 O.A.C. 125, at para. 39; Slocan Forest Products Ltd. v. Trapper Enterprises Ltd., 2010 BCSC 1494, 100 C.P.C. (6th) 70, at para. 15. The parties’ ability to confidently develop strategies knowing that they cannot be compelled to disclose them is essential to the effectiveness of this process. In Quebec, as in the rest of the country, litigation privilege is therefore inextricably linked to certain founding values and is of fundamental importance. That is a sufficient basis for concluding that litigation privilege, like solicitor-client privilege, cannot be abrogated by inference and that clear, explicit and unequivocal language is required in order to lift it.

Considering the current state of the law, the university recommends that the *Act* be amended to include clear and unambiguous language that the Commissioner is not entitled to compel records or information that is protected by solicitor-client or litigation privilege. The provision should expressly stipulate that the Commissioner cannot compel production of solicitor-client and litigation privileged records in the course of an access complaint investigation as they are protected by s. 30, and that the burden of proof in claiming such privilege is based on the civil law standard.

In making this submission, Memorial University would ask that the Commissioner's role be taken into consideration. Memorial has processed many requests over the years that involved solicitor-client and/or litigation privileged records that were the subject of ongoing ATIPP-related disputes. Production of those records to the Commissioner in the context of their role as a decision-maker, and party to ATIPP Appeals, would be fundamentally unjust.

It is also worth noting that over the course of many complaint investigations with the University, some of which have resulted in the issuance of a formal report (e.g. A-2020-008, A-2020-017), the OIPC has continuously accepted a description or listing of solicitor-client and/or litigation privileged information with submissions as to why such information is privileged, in lieu of production of the privileged records themselves.

Recommendation #3

The university recommends codification of the current state of the law in this province regarding solicitor-client, and litigation privileged records, and production of these records to the commissioner. Specifically, the university recommends the addition of explicit language stating that the Commissioner may not compel production solicitor-client and/or litigation privileged records; and further, that a public body has discharged its burden by complying with the civil standard in litigation by identifying privileged documents, asserting a claim for privilege, and noting the type of privilege applied.

Recommendation 4: Exception to Access – s. 33 Workplace Investigation

Our Justification

Memorial has received and processed a number of requests pursuant to section 33 of the *ATIPPA, 2015*. Section 33 is somewhat unique in Canada:

33. (1) For the purpose of this section

(a) "harassment" means comments or conduct which are abusive, offensive, demeaning or vexatious that are known, or ought reasonably to be known, to be unwelcome and which may be intended or unintended;

(b) "party" means a complainant, respondent or a witness who provided a statement to an investigator conducting a workplace investigation; and

(c) "workplace investigation" means an investigation related to

(i) the conduct of an employee in the workplace,

(ii) harassment, or

(iii) events related to the interaction of an employee in the public body's workplace with another employee or a member of the public which may give rise to progressive discipline or corrective action by the public body employer.

(2) The head of a public body shall refuse to disclose to an applicant all relevant information created or gathered for the purpose of a workplace investigation.

(3) The head of a public body shall disclose to an applicant who is a party to a workplace investigation the information referred to in subsection (2).

(4) Notwithstanding subsection (3), where a party referred to in that subsection is a witness in a workplace investigation, the head of a public body shall disclose only the information referred to in subsection (2) which relates to the witness' statements provided in the course of the investigation.

From our significant experience with ATIPP requests pertaining to workplace investigations, a shortcoming of the *ATIPPA, 2015* has been observed, specifically the lack of a time limitation placed on disclosure prior to the investigator's report being issued. Therefore, a party to a workplace investigation can request all records relating to the investigation, including from the other party and the investigator, before the investigator has even concluded their investigation and produced their report. Not only does this render consideration of what records are "relevant" to the investigation cumbersome, but it challenges the integrity of an investigation and places unnecessary stress on the other party and the investigator as they are trying to conduct their work. A relationship between the parties is already strained by the time an investigation is reached, and submitting an ATIPP request requiring the other party to compile and provide all records relating to the investigation before the matter has been completed adds further strain on an already tense situation. It can also serve to antagonize the other party to the investigation, to the detriment of the investigation and ultimately the workplace relationship. A workplace investigation, by default, provides a communication channel via the investigator for evidence to be presented and shared and for the parties to respond accordingly. Processing an ATIPP request about an investigation, while at the same time conducting that investigation, is not an efficient use of resources and, more to the point, may frustrate the aims of the investigation. Workplace investigations conducted under relevant University policies are designed to ensure they meet legal standards of procedural fairness and natural justice and the parties to an investigation have an opportunity to respond to an investigation report upon receiving it.

Memorial submits that disclosure of records under section 33 should await the conclusion of the investigation and issuance of the investigator's report. Amending the legislation to prevent disclosure prior to an investigator's report being issued is in the interest of the parties to a workplace investigation, the investigator and the employer, and also would serve to support more efficient use of public body resources.

Recommendation #4

Memorial University recommends that an amendment to section 33 provide that records pertaining to a workplace investigation be withheld until *after the investigator's report has been issued*.

[Recommendation 5: Limit on Concurrent Access Requests from the Same Applicant](#)

Our Justification

The current statute contains no limitations on the number of access requests an individual may make to a public body at the same time. As such, it is not uncommon for Memorial University to receive multiple concurrent access requests from the same ATIPP applicant, which are at times for similar or related records.

The absence of a restriction on the number of allowable concurrent requests presents several operational challenges for the University, primarily in our ability to meet statutory deadlines in collecting and processing records.

Furthermore, the absence of a provision to limit multiple concurrent requests enables individuals to make regular systematic requests, or requests otherwise made in bad faith, which ultimately amounts to an abuse of process of the legislation, as delineated by s. 21 of the *ATIPPA, 2015*. The university has direct experience of managing multiple systematic requests from the same applicant. It is also unfair to the applicants of other ATIPP requests as one single applicant who files multiple concurrent requests consume a significant amount of public body resources to process their multiple requests, thereby leaving less time to process the requests filed by other applicants.

In an effort to mitigate a potential abuse of process and to ensure the efficient and timely processing of access requests, we recommend that the legislation be revised to limit the total number of concurrent access requests an individual may make.

We note that pursuant to subsections 44(7) and 74(4) of the *ATIPPA, 2015*, concurrent access and privacy complaints by the same applicant in excess of five may be held in abeyance until the Commissioner has responded to one of the maximum allowable complaints. It is reasonable that the public body should have the same protection against multiple concurrent requests as the Commissioner.

Recommendation #5

Memorial University recommends a limit on the number of concurrent requests made by the same applicant.

Recommendation 6: Fee Considerations

Our Justification #1

Section 25

The university believes an application fee for making an ATIPP request should be restored. An application fee lends *gravitas* to an applicant's decision to file a request for access to public body records and ensures that applicants consider carefully the nature of their request and the decision to file an ATIPP request, rather than seeking the information through other informal channels. Ultimately, the fee may help to reduce poorly-considered, repetitive, vexatious or frivolous requests.

Memorial University submits further that s. 25 (3) of the *ATIPPA, 2015* should be amended to include expanded grounds on which an applicant may be charged fees connected with processing access requests. At this time, fees can be charged only for "locating" records (see the Guidance published by the OIPC in this connection: <https://www.oipc.nl.ca/pdfs/CostEstimates.pdf>). As a result, in contrast with the previous ATIPP legislation, under the *ATIPPA, 2015* Memorial University rarely issues fee estimates for ATIPP requests. In particular, we submit that a public body should have the opportunity to charge fees not only for locating a record but also for the services of identifying, retrieving and compiling records. This challenge is highlighted, in particular, in connection with requests for information located in databases. Such requests are dealt with under ss. 20(2) and (3). However, we wish to note that providing information from databases is not an automatic exercise. Requests are rarely, if ever, straightforward and rarely for reports that are regularly and ordinarily produced from a database for internal operational purposes. Instead, such requests often require multiple senior analysts to develop custom queries for multiple databases in order to assemble the precise information sought in an ATIPP request. That information must then be studied for verification and reconciliation. While ss. 20(2) and (3) do helpfully state that such requests need be answered only if they can be answered using the public body's normal hardware, software and expertise and doing so would not unreasonably interfere with operations, that is not the complete answer to the issue. In practice, neither the ATIPP coordinator nor the analyst(s) involved will have insight into what challenges retrieving the information might present. By the time the complexity and resources required are determined, the analysts and experts have already invested hours of time and the public body does not wish to advise the applicant that their request cannot be accommodated.

The processing of an ATIPP request at Memorial University involves a multi-faceted response as requests frequently require the IAP Office to engage with offices and units University-wide in the search

and location of responsive records. Searches for records are conducted by employees who are familiar with the records requested, as per s. 11(2)(b). From a procedural standpoint, upon receipt of an access request, the IAP Office sends the wording of the request, along with guidance on how to conduct a search for records and a “Locating Records Worksheet” to employees who will administer a search for records. These employees are asked to provide an estimate of the time they anticipate it will take to locate records responsive to the request.

The provision of an estimate of search time by employees who will carry out the search is a crucial component in the processing of an ATIPP request, as it provides insight to the IAP Office on the total number of hours expected to locate records and, in turn, whether an Estimate of Costs to an applicant is warranted.

The “Locating Records Worksheet”, on the other hand, is to be completed once a search for records has been fully executed and the records submitted to the IAP Office for processing and redaction. The Worksheet indicates the total time taken to locate responsive records, as well the time spent in identifying, retrieving, reviewing, photocopying and scanning the records. This process assists the university in monitoring resources expended in complying with ATIPP requests.

What we have come to learn is that the bulk of the time spent by employees conducting searches for records pertains not to the locating of records but to the “other” aspects of responding. This is due, in large part, to the speed at which an electronic search can be executed. While a quick key word search to “locate” records may take only minutes, it can take employees many hours to identify, review, extract, scan, copy and internally review records that have been “located” as a result of a key word search. Many of the records located as a result of the key word search may not even be relevant to the request. Non-responsive records must be vetted by those conducting the search before responsive records are sent to the IAP Office and, as is often the case, the responsive records provided to the IAP Office are further analyzed and vetted by the IAP Office. Effectively, the *ATIPPA, 2015*’s provision for 15 hours of free time locating records before a Cost Estimate can be considered does not consider modern electronic storage of information.

While operationally the University continues to rely to some degree on the use of paper records, the majority of communications and the transfer and sharing of documents are executed by way of electronic means.

Physical searches, although less frequent, can require exorbitant hours of employee time and resources, as in addition to the physical search itself, these same “other” aspects of the search must be completed prior to submission of the records to the IAP Office.

For these reasons, we recommend the legislation restore an application fee and broaden the basis on which an estimate of costs may be considered by including time taken by employees in fully executing records searches and the time required to extract and assemble accurate information from databases.

We make this recommendation not to deter an applicant's right to request access to information, but to encourage applicants to make their requests thoughtfully and to limit the constraints on the offices and units within the public body that are required to allocate, on occasion, substantial time and resources to fully execute records searches and assemble records in response to requests.

Further, having even a modest fee would discourage repetitive or systematic requests, or abuse of the ATIPP process. The university has a number of very frequent ATIPP requestors. One in particular has made close to 450 requests, many of which are repetitive and systematic, and some of which are vexatious. Even a modest fee of \$5 per request might help ensure that the process is being used as it was designed, and not simply as a way to frustrate resources.

Given the above, it is recommended to have an application fee and amend ss. 25(3) to permit charges for certain types of activities.

Our Justification #2

Section 26

Pursuant to s. 26, upon the issuance of an Estimate of Costs to an applicant, the applicant is provided four options: accept the fee, modify the request, withdraw the request, or ask for a waiver of fees. The applicant has a full 20 business days to consider and respond to the Estimate, including to apply to the Commissioner to revise the Estimate. The powers of the Commissioner in connection with Fee Estimates are contained entirely in s. 26(7) and (8). Subsection 26(9) states that a public body shall comply with a decision of the Commissioner under this Section. Furthermore, ss. 42(8)(d) states that a Fee Estimate shall not be the subject of a Complaint to the Commissioner. In recognition that the Commissioner's decision under s. 26 is final, the *ATIPPA, 2015* further states in s. 55 that an estimate of costs or a decision not to waive a cost under s. 26 cannot be appealed to Court.

Notwithstanding the above, the Commissioner did recently undertake a Complaint investigation about a fee that was paid by an applicant to Memorial University. Despite representations by Memorial that the applicant paid the fees, the request was processed and notwithstanding that a Complaint about it could not be undertaken pursuant to s.26 and s.42, the Commissioner did investigate. See Report A-2019-032, available at <https://www.oipc.nl.ca/pdfs/A-2019-032.pdf>. In the Report, on the subject of its jurisdiction to investigate a complaint about fees, the Commissioner stated, "there is some ambiguity in the Act." Memorial submits there is no ambiguity in the Act. However, as the Commissioner has suggested there is, Memorial submits that any perceived ambiguity should be resolved and asks you to consider the following perspective.

By granting a full 20-business day period for an applicant to consider a Cost Estimate and to also ask for a review of the Cost Estimate by the OIPC, the intent of the legislation is for s. 26 to dispense with all issues, including OIPC reviews. The legislature clearly intended that once a Cost Estimate is accepted, modified, or revised by the Commissioner under s. 26, the matter is final and, at that stage, a public body may proceed to process a request.

Given the above, it is recommended to clarify in s. 26 that the Commissioner's decision under s. 26 is final and cannot be the subject of a Complaint under s. 42 or appeal to Court under s. 55.

Recommendation #6

Memorial University recommends:

- The restoration of an application fee
- Amendment of s. 25(3) to permit charges for certain types of activities
- Clarification in s. 26 that the Commissioner's decision under s. 26 is final and cannot be the subject of a further Complaint to the Commissioner or appeal to Court under s. 55.

Recommendation 7: Record(s) already possessed by an Applicant

Our Justification

Two of the *ATIPPA, 2015's* purposes are:

1. Ensuring that citizens have the information required to participate meaningfully in the democratic process, and;
2. Increasing transparency in government and public bodies so that elected officials, officers and employees of public bodies remain accountable.

Providing record(s) that an applicant already possesses is redundant, wasteful and does not further the purposes of the legislation. The applicant already has the records to participate meaningfully in the democratic process and to increase transparency in government and public bodies. Submitting an access to information request to a public body for these same records does not achieve these purposes and is not in the public interest. It wastes valuable public body resources, particularly in times of budget constraints, and can diminish the legitimate access rights of others.

Applicants requesting records they already possess have proven to be a vexatious problem for Memorial, whether it be for emails they already received, emails they generated, emails they were copied on, or for other materials they submitted to the University. Memorial has had requests for emails that were sent to the applicant by Memorial employees, emails that they were copied on and, indeed, emails they authored.

This also presents an issue when applicants file numerous requests to the same department in respect of a particular project. When records are provided by the department to the ATIPP coordinator, it becomes apparent that the applicant already possesses some of the records. However, in accordance with the *ATIPPA, 2015* whether or not the applicant already has them, they must be provided to the applicant. Indeed, the university has had experiences where the OIPC, in undertaking a complaint

investigation under s. 42, has conceded that the complainant has the records but nevertheless insisted that Memorial provide them to the complainant-applicant.

Processing records an applicant already possesses via an ATIPP request erodes the importance and value of the *ATIPPA, 2015*. This is particularly evident in a personal information request where employees searching for records must know the name of the applicant in order to locate records containing the applicant's personal information. There have been many instances where the individuals conducting the search know for certain the applicant already possesses the records, whether that be through their employment or because they were sent or copied on emails. Offices that must provide these same records question why it must be done, express how vexatious it is, and sometimes question the value of the *ATIPPA, 2015* as they experience it being used as a form of nuisance or harassment. When individuals are already experiencing a high workload in their own office duties, having to search for and provide records which they know the applicant already has, appears senseless and is exhausting, as it requires them to carve out time in their already busy schedule to conduct this work. This erodes the confidence of employees of public bodies in what should be a valuable and critically important tool for transparency.

Memorial submits the *ATIPPA, 2015* should be amended to permit a public body to refuse to provide records where there is evidence that the applicant already has them in their possession.

Recommendation #7

Memorial University recommends that the *ATIPPA, 2015* should be amended to permit a public body to refuse to provide records where there is evidence that the applicant already has them in their possession.

[Recommendation 8: Preventing Abuse of the *ATIPPA, 2015* – s. 21 Disregarding a Request](#)

Our Justification

The public's right to access information held by public bodies plays an important role in promoting democracy. However, as recognized by section 21 of the *ATIPPA, 2015*, the right of access presents an opportunity for abuse. It can, and does, take various forms, including where the applicant attempts to dictate the process, or act as a management surrogate; when requests are filed for an improper objective such as harassing a public body or its employees; and when requests are used as a weapon against a public body, or to commit what the jurisprudence refers to as information warfare. Such abuse of the right of access has serious consequences. The misuse of the legislation brings the *Act* into disrepute and "can threaten or diminish the legitimate exercise of that same right by others." It "also harms the public interest, since it unnecessarily adds to the public body's costs of complying with the *Act*." Unfortunately, Memorial University has had experiences with vexatious applicants and both of these consequences.

In Memorial's experience, the legislation has been used as, amongst other things, a form of bullying and harassment. This has manifested itself as years of targeted requests, numerous applications to the Office of the Information and Privacy Commissioner for approval to disregard abusive requests, to which approval was granted in most cases, and a plethora of Court actions. A significant example of this abuse of the legislation was acknowledged by the Supreme Court of Newfoundland and Labrador in *Memorial University of Newfoundland v. Oleynik*, 2024 NLSC 42 where the ATIPP applicant was declared a vexatious litigant. The Court fell short of declaring the individual a vexatious ATIPP applicant as the Court noted that, as the legislation was currently written, "it does not have the capacity to impose a policy decision, even one which may be preferable, within the sphere of authority constitutionally provided to a legislature. It is essential to ensure that sufficient deference is paid to legislative intent." While the court was required to stop short of formally declaring the applicant a vexatious ATIPP requestor, the court nonetheless carefully pointed out that all of the vexatious behaviours engaged in by the applicant toward the courts, were also engaged in through their abuse of the ATIPPA process. The Court made some noteworthy statements in their decision regarding both the vexatious litigant and vexatious ATIPP applicant piece, as cited below:

[6] *This case is a remarkable example of such an abusive litigant.*

...

[11] *It is a difficult task to summarize the many proceedings, judicial and otherwise, Oleynik has brought against Memorial in a manner which would reveal a coherent narrative. Regardless, even a cursory review of the various applications and processes initiated against Memorial gives rise to the compelling suggestion that Oleynik is not interested in obtaining a remedy or relief but rather is attempting to use this Court as a weapon in his crusade against Memorial. And further, it suggests that the whole of these proceedings has been a disingenuous and relentless attempt to bring Memorial to its knees driven by Oleynik's delusionary view that a great wrong will be revealed.*

...

[68] *Oleynik continually raises issues that have already been decided. There are several written decisions of this Court which highlight this fact (Oleynik, 2023 NLSC 86 at para. 132), thus there is no need to undergo a forensic reconstruction of every such inappropriate instance. Also, Memorial in its brief at pages 30 to 33 does a comprehensive job of providing specific examples which serve to demonstrate Oleynik's pattern of raising issues already determined, his lack of respect for rulings made against him, and for the authority of the Court more broadly.*

...

[80] *The evidence is abundantly clear that Oleynik sought to use his legal proceedings, not only to challenge decisions made at Memorial with which he disagreed but also to make baseless accusations and raise conspiracy theories first against Memorial officials, before progressing to court staff, and eventually judges, and to make further complaints of professional misconduct to the Law Society and allegations of criminal actions to the RNC*

...

[83] Perhaps the most obvious example of the vexatious manner in which Oleynik has conducted his litigation is his practice of rolling past or present proceedings into subsequent proceedings. Oleynik deliberately structures his claims so that they mushroom outwards, using and abusing statutory decision-making bodies to create a multiplicity of different actions.

...

[85] To understand Oleynik's *modus operandi* it first must be recognized that each request for information under ATIPPA initiates a distinct administrative proceeding and response from the public body. Two apparently related proceedings are, by merit of being requests having been made at different points of time, separate proceedings under ATIPPA. Oleynik will make an ATIPP request to Memorial, following which he will make a formal complaint to the Privacy Commissioner that the response is inadequate. Following this, he will appeal the action taken by Memorial, regardless of whether or not they complied with the Privacy Commissioner's report. Alternatively, he may appeal Memorial's decisions directly to the Court and bypass the Privacy Commissioner complaint process. Thereafter, Oleynik will make a second request for information, focusing on Memorial's response to the first request. The second response generated by Memorial will then be the subject of a complaint to the Privacy Commissioner and further appeal to this Court. It should be recognized that when Oleynik requests all records responsive to an issue and then makes the same or substantially similar request at a later date, the second request generates a duplication by Memorial of the records responsive to the first request plus any additional information. The process is then repeated by Oleynik regarding a separate issue or compounding the first issue into multiple ATIPPA requests. As a result of Oleynik's actions through this repetitive and tactical approach to ATIPPA, he creates a pyramid of administrative reply from the public body (Memorial) and from the Privacy Commissioner together with litigation on all fronts.

...

[106] I declare Oleynik a vexatious litigant. The following facts, *inter alia*, have lead me to this conclusion:

...

- Oleynik has trafficked in conspiracies and unfounded allegations of misconduct and bias for which there is no evidential basis, and has repeatedly made these assertions to the Court as grounds for which the orders he seeks should be granted;
- Oleynik's true purpose, if it can be said that he has ever had one, has long become lost in his efforts to use the judicial process to harass Memorial, its employees, and its counsel;

...

[116] There is compelling evidence that Oleynik has acted in much the same way regarding [ATIPPA](#) as he has in his applications before this Court: namely, that his requests for information are often frivolous or vexatious, frequently repetitive and systematic in their approach,

excessively broad, and otherwise made in bad faith. The Privacy Commissioner does not dispute this position and acknowledges that many requests for information were rightly disregarded by Memorial.

We note that the above-noted decision has been upheld by the Newfoundland and Labrador Court of Appeal, and the ATIPP applicant's application for leave to appeal to the Supreme Court of Canada has been refused.

A consequence of the above-noted abuse is that some members of the public body now question the legitimate exercise of the right of access by others. Maintaining cooperation from public body employees is essential to ensure statutory obligations are upheld. Memorial University has noted a dramatic increase in the amount of resources needed, both financially and in terms of human resources, to respond to frivolous and vexatious requests and consequent complaints and appeals. Increased safeguards are warranted and needed.

Abuse of the legislation is currently guarded against by section 21 of the Act. It states:

21. (1) The head of a public body may, not later than 5 business days after receiving a request, apply to the commissioner for approval to disregard the request where the head is of the opinion that

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

(2) The commissioner shall, without delay and in any event not later than 3 business days after receiving an application, decide to approve or disapprove the application.

(3) The time to make an application and receive a decision from the commissioner does not suspend the period of time referred to in subsection 16 (1).

(4) Where the commissioner does not approve the application, the head of the public body shall respond to the request in the manner required by this Act.

(5) Where the commissioner approves the application, the head of a public body who refuses to give access to a record or correct personal information under this section shall notify the person who made the request.

(6) The notice shall contain the following information:

- (a) that the request is refused because the head of the public body is of the opinion that the request falls under subsection (1) and of the reasons for the refusal;*
- (b) that the commissioner has approved the decision of the head of a public body to disregard the request; and*

(c) that the person who made the request may appeal the decision of the head of the public body to the Trial Division under subsection 52 (1).

Memorial University is respectfully of the view that this section is ill-equipped to adequately guard against abuse of the legislation and, in particular, repetitive abuse.

The Problems with Section 21

(a) The Time-Frame for Determining Whether a Request is Abusive: Section 21(1)

The time-frame for filing an application to disregard in subsection 21(1) is prohibitive. In many cases, either because of the wording of the request and/or input needed from employees who possess records, an ATIPP coordinator may not appreciate the vexatious or frivolous nature, bad faith, or interference that underscores an access to information request until after the deadline for filing has passed. A longer time-frame for determining whether a request is an abuse of the legislation is warranted for the following reasons:

1. Requests have become larger, more complex and in some cases excessively broad. Members of the public are increasingly informed about access to information legislation and their right to request records held by public bodies. This is a great success of the *ATIPPA, 2015*. However, as individuals are increasingly engaged, so too are the depth and scope of the topics on which they seek information. As a result, a public body often requires significant time to review a large, complex and/or excessively broad request to determine whether it is reasonable to process or whether, after efforts to focus and scope the request with an applicant have failed, the public body must proceed with preparing a disregard submission. The 5 business day timeline to disregard a request does not reflect this trend of larger and more complex requests filed by applicants. It also does not give time for the public body to attempt to scope an overly broad or unclear request prior to making a decision about applying to the Commissioner to disregard the request.
2. The level of effort required to assess reasonableness of a request. To truly understand the scope of a request, the ATIPP coordinator must contact the department(s) and/or individual(s) who would need to conduct the search for records to discuss what the request is seeking. This is particularly true for Memorial, which is a large, multi-campus university community that includes students, faculty, staff, researchers and alumni. New and innovative initiatives and activities regularly happen at the university and these prompt ATIPP requests, requiring the ATIPP coordinator to obtain background information from applicable units and individuals in order to understand the scope of the request, determine whether the records are within the custody and control of the university, possibly seek legal advice, and determine the reasonableness of the request under s.21. The 5-business day timeline to seek authorization to disregard a request does not provide adequate time for this level of effort.

3. The necessity to disregard a request is not evident until records are reviewed. Many employees, when receiving notification that they must search and provide records for an ATIPP request, will gather all of the records and submit them to the ATIPP coordinator. They may not be inclined to question whether the request should be disregarded. In most cases, it is not until the ATIPP coordinator reviews the records that it becomes evident that a disregard submission should have occurred, but by the time the records are provided and reviewed the deadline has often passed. One of the grounds on which a request may be disregarded is ss. 21(1)(b): the request is for information already provided to the applicant. Again, the records must be reviewed to determine if some or all of them have already been provided to the applicant. This leaves a public body to complete a request which ought to have been disregarded on the basis of one or several of the grounds in section 21. Consequently, other ATIPP requests are impacted and not responded to as quickly.
4. The level of effort required to prepare an application to disregard. A disregard application requires significant effort. The University Privacy Officer must first analyze the request in light of the statutory grounds to request a disregard, then prepare a draft submission and conduct necessary internal, and sometimes external, consultations prior to submitting. This all has to occur within 5 business days. To persuade the Commissioner that a disregard is warranted, the application to disregard usually must cover all applicable grounds. When a disregard application is determined to be necessary, all other access and privacy work must essentially cease in order to allow time to be able to analyze the request in light of the enumerated grounds, draft a submission, conduct research into case law, review prior OIPC reports, and conduct consultations on the submission. Furthermore, both internal and external legal counsel often need to be consulted on account of ATIPP requests pertaining to litigation or disputes. Submissions must be approved by senior administration. The 5-business-day timeline does not reflect the sheer amount of effort required by a public body to prepare, draft, conduct research, consult and finalize a formal disregard submission for the Information and Privacy Commissioner.

(b) The Time-Frame for Responding to the Request: Section 21(3)

The requirement imposed by subsection 21(3) to complete the request within the original deadline in the event that the application to disregard is unsuccessful is also problematic. Subsection 21(3) requires a public body to continue to process the request, e.g., collect responsive records, while preparing an application to disregard and awaiting a decision from the Information and Privacy Commissioner. This is onerous, and it means that the harm that a public body seeks to avoid by an application to disregard is still incurred. For example, if the legislation is being used as a form of harassment, requiring those employees who feel harassed to nevertheless search for records in the interim period enables the harassment. It also can be perceived as callous and, like all forms of abuse, undermines respect for the legislation and the importance of the right of access.

(c) An Absence of Procedural Fairness

Under section 21(2), the Information and Privacy Commissioner has three days to make a decision on an application to disregard. There is no opportunity for an access to information applicant to make submissions on the application. Nor does the Commissioner have an opportunity to complete an investigation or render a report on its findings. Its decision is not shared with the applicant, nor is it made public. The public body receives a decision on its application to disregard. If the disregard is approved, the public body must then inform the applicant. The applicant is given an opportunity to appeal – but not the decision of the Commissioner, as that is not shared with the applicant, pursuant to s. 41(c). The applicant has to appeal the decision of the public body to disregard, without ever having seen the public body's submissions to the Commissioner or the Commissioner's decision. As a result, there is a lack of procedural fairness, transparency in the process and reportable decisions which could provide precedents and guidance on the abuse and appropriate use of the *ATIPPA, 2015*. With these limitations is an increased propensity for disregard decisions to be appealed to Court under subsection 21(6)(c), thereby increasing the costs to the public body and the courts.

(d) The Absence of Effective Remedial Authority

Subsections 21(1), (4) and (5) refer to “the request.” This has been interpreted by the Information and Privacy Commissioner as a limitation on their remedial authority, specifically that the Commissioner can only address individual requests on a case-by-case basis. This limitation fails to remediate repetitive abuses of the legislation and the harms outlined above. The authority to craft a remedy that is proportionate to the harm conducted and the mischief that the section seeks to guard against, and should guard against, is notably absent.

(e) The Right of Appeal and the Process

Under section 21(4) of the current legislation, a public body is required to respond to an access to information request where the Information and Privacy Commissioner does not approve an application to disregard. There is no provision for the public body to advance its case to the Supreme Court of Newfoundland and Labrador if it disagrees with the Commissioner's decision. This limitation fails to take into account the conflict between the dual role of the Commissioner as an advocate for access pursuant to sections 3(1)(f)(a), and as a quasi-decision-maker under the legislation. It serves as a barrier to access to justice for a public body. The public body ought to be afforded the same right as an applicant to be able to advance its case to the Supreme Court if necessary.

Additionally problematic is the role of the Information and Privacy Commissioner, or lack thereof, on an appeal of a decision to disregard. Under subsection 56(4)(a) the Commissioner is not permitted to intervene as a party to an appeal in respect of a decision to disregard a request. The consequence is that the entity tasked with independent oversight of the legislation

is not permitted to make submissions to the Court on what constitutes an abuse of its own legislation, even though it has already provided a written decision on the exact issue to the public body. While the Commissioner is not a typical decision-making body due to its advocacy for access role and its quasi-order making power/recommendation-making power, this limitation on the Commissioner's ability to provide input and assistance to the Court is out of step with jurisprudence where the Court seeks to exercise its inherent jurisdiction to prevent abuses of subordinate legislation. The current process also lacks procedural fairness as the parties are left to argue the disregard matter without reference to the decision with reasons, provided by the Commissioner. This means there is no opportunity for the court to consider what level of deference is due the Commissioner when it provides its disregard decision to the public body.

There is currently inefficient and insufficient oversight of abuses of the *ATIPPA, 2015*. Section 21 should be amended to better prevent abuses of the legislation and to give remedial effect to that purpose. In this respect, Memorial University recommends that:

(i) Newfoundland and Labrador adopt the approaches of other Canadian provinces, which allow a public body to decide on its own, without the Commissioner's approval, to disregard a request. This is the case in Ontario, where a public body can disregard a request that is an abuse of the legislation without approval from the Information and Privacy Commissioner. In 2024, Alberta's access to information legislation was updated and now includes a provision to allow the public body to make its own determination to disregard a request based on criteria similar to our s. 21; the public body is granted 30 business days to advise the applicant of their decision to disregard, and the applicant may request a review of the disregard.

Similar amendments to the *ATIPPA, 2015* would have the effect of precluding harm that is currently sustained while an application is being prepared and a decision is pending on an application to disregard, and should be considered in combination with recommendation (ii).

(ii) An applicant ought to be permitted to complain to the Information and Privacy Commissioner about, or appeal directly to the Supreme Court about, a public body's decision to disregard a request. The Commissioner should have an opportunity to investigate and prepare a Report. The Report should be provided to both the public body and the applicant, and there should be an opportunity for either party to appeal a Report of the Information and Privacy Commissioner to the Supreme Court. This would enhance procedural fairness and transparency, provide precedents and education on the abuse and the proper uses of the *ATIPPA, 2015*, and provide the public body with an opportunity to appeal a decision of the Commissioner regarding abuse of the legislation. It would also bring the review process for disregards, in line with the review / appeal process that otherwise applies under the current regime.

(iii) The Information and Privacy Commissioner and the Supreme Court of Newfoundland and Labrador ought to have the remedial authority to craft a remedy that is necessary to rectify and

prevent the harm caused by abuse of the legislation, such as placing restrictions on an applicant's ability to file requests, and declaring someone a vexatious applicant for abuse of the legislation through any of the statutorily enumerated forms of abuse.

(iv) In addition to the foregoing, there should be a separate and independent provision enabling a public body to apply to both the Information and Privacy Commissioner or the Supreme Court of Newfoundland and Labrador to have someone declared a vexatious applicant for abuse of the legislation. This would preclude the necessity of an applicant filing a complaint or appeal regarding a disregard, in order for a public body to advance a declaration application on its own merit.

(v) The Information and Privacy Commissioner ought to have a right of intervention on an appeal to Court regarding a decision to disregard a request, or an application to Court to have someone declared a vexatious applicant.

Recommendation #8

Memorial University recommends that Section 21 be amended to provide better oversight of abuses of the legislation and to give remedial effect to that purpose.

Recommendation 9: Duty to Assist

Our Justification

The duty to assist is contained in section 13 of the *ATIPPA, 2015*. It states:

13.(1) The head of a public body shall make every reasonable effort to assist an applicant in making a request and to respond without delay to an applicant in an open, accurate and complete manner.

(2) The applicant and the head of the public body shall communicate with one another under this Part through the coordinator.

The duty to assist is the only obligation of the head of a public body that is characterized as a "duty" under the Act. It is referenced in only two other sections of the Act – s.95 and s.105:

Ss. 95(2)(b) – that the Commissioner shall develop and deliver an educational program that shall include informing public bodies of their duty to assist,

Ss. 95(2)(h) – that the Commissioner shall bring to the attention of the head "a failure to fulfil the duty to assist applicants"

S. 105 – where the Commissioner shall in its annual report to the House of Assembly note “persistent failures of public bodies to fulfil the duty to assist applicants.”

The legislation does not prescribe how the Commissioner should bring a failure of the duty to assist to the attention of the head. We note that it has been a common practice for the OIPC to accept complaints regarding the duty to assist.

Three sections of the Act address the circumstances in which a public body is required to notify a requester or third party of their right to file a complaint under s. 42:

Ss. 17(1)(c)(ii) where access to a record or part of a record is refused

Ss. 18(1)(b)(iii) where a request for correction of personal information is refused

Ss. 19(5)(c) and 19(6) concerning access to third party information

No section of the Act requires a public body to provide applicants with notice of their right to lodge a Complaint under section 42 for alleged breaches of the duty to assist.

The Information and Privacy Commissioner has interpreted section 13 as requiring, *inter alia*, a reasonable search for records. As a result, where the Commissioner is of the view that a reasonable search has not been conducted, they have recommended further searches. For instance, in Report A-2019-018, the Commissioner recommended as follows:

[48] Further we recommend follow up questions regarding the search be sent, in writing, to the Office of the Provost and to the investigator asking specifically that all paper records be searched, including notebooks and files and that any records found be released to the Complainant, subject to appropriate redactions.

At best, a recommendation to conduct a further search for records falls within section 47(d) of the legislation, which states:

47. On completing an investigation, the commissioner may recommend that
(a) the head of the public body grant or refuse access to the record or part of the record;
(b) the head of the public body reconsider its decision to refuse access to the record or part of the record;
(c) the head of the public body either make or not make the requested correction to personal information; and
(d) other improvements for access to information be made within the public body.

In light of the above, we recommend an amendment to s. 13 of the Act to provide prescriptive clarity surrounding the obligations of the public body as it pertains to the duty to assist an applicant.

Recommendation #9

Memorial University recommends clarification on the review process and enforcement in respect of the duty to assist, taking into consideration:

- (a) the costs of compliance
- (b) timely access
- (c) the need for finality of the process

Recommendation 10: Protection for IT Security Arrangements

Our Justification

Subsection 31(1)(l) is a discretionary exception to disclosure that permits a public body to withhold, among other things, information that would reveal security arrangements. It states:

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

(l) reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;

Memorial recommends strengthening subsection 31(1)(l) so that information revealing information security, cybersecurity, cloud security, identity and access management and digital infrastructure is protected where disclosure could reasonably be expected to increase cybersecurity risk. The current discretionary exception does not adequately account for the cumulative value of technical and operational details that may appear innocuous in isolation but can be combined to identify vulnerabilities, target privileged users, or compromise interconnected systems. The purpose of the amendment is to protect the confidentiality, availability and integrity of critical infrastructure, public-sector systems/services and the information entrusted to public bodies.

Three features of the university environment increase the consequences of disclosing information about IT security arrangements:

1. Universities have a large and diverse threat surface because their teaching, research and administrative activities depend on open collaboration and broad access. Memorial's user community and institutional relationships extend worldwide, increasing the number and variety of potential points of entry.
2. Memorial University operates one of the largest IT environments in the province and is connected to the provincial government, regional health authorities, national and international networks, other universities and major private organizations. Because these systems and relationships are interconnected, a major security breach at Memorial could have far-reaching consequences for both Memorial and non-Memorial entities.

3. Canadian federal cybersecurity organizations, including the Canadian Centre for Cyber Security, have warned universities, including Memorial University, that threat actors actively attempt to infiltrate Canadian universities and other public and private-sector organizations.

Technical and operational information can be combined and used to support cyberattacks:

1. The cyber threat landscape continues to evolve rapidly. Artificial intelligence is enabling threat actors to operate more quickly and at greater scale, produce more convincing phishing and impersonation attempts, automate elements of reconnaissance, and identify or exploit vulnerabilities more efficiently. These developments reinforce the importance of protecting technical and operational information that could support AI-assisted targeting.
2. Social engineering is when information is slowly and carefully gathered from multiple sources using various approaches until the attacker has enough intelligence gathered to perform the targeted attack. Disclosing details about operating systems, software versions, patch levels and identity of system administrators gives attackers detailed information that can be used in a cyber-attack. For example, with a system administrator's name in hand, an attacker can send spoof emails using the actual name, a much more effective tactic for a cyber-attacker than using a generic title System Administrator.
3. Privileged accounts are particularly valuable targets because they provide extensive control over networks and systems. The Canadian Centre for Cyber Security explains the associated risks in its video on administrative privileges: <https://cyber.gc.ca/en/administrative-privileges>. Attackers may exploit technical vulnerabilities or use stolen credentials to obtain elevated access and move through an organization's environment. Comparable incidents have occurred at numerous [universities](#). Microsoft identifies these accounts as especially attractive targets for credential theft: [Attractive Accounts for Credential Theft | Microsoft Learn](#).

The consequences of a successful cyberattack are not theoretical. Memorial University experienced a significant cybersecurity attack at Grenfell Campus in December 2023. Memorial's IT team and contracted third-party cybersecurity experts worked extensively to restore services and guide the university through the incident, as summarized here: <https://gazette.mun.ca/campus-and-community/setting-the-bar-2/>. The attack disrupted communications, teaching and research tools, and access to information at Grenfell Campus. The response required nearly continuous work during the initial days and weeks to restore sufficient technology services to the campus to reopen, initially with limited functionality.

Memorial University continues to be a frequent target of cyberattacks. Its security controls regularly detect and block thousands of malicious events and attempted intrusions, millions of malicious email messages, and much larger volumes of unwanted network connection attempts.

How disclosure under ATIPPA can increase cybersecurity risk:

Information disclosed through separate ATIPP requests can be combined to create a detailed picture of a public body's security environment. Software versions, patch levels and the names of system or network administrators may appear limited when considered individually, but together they can help attackers identify vulnerabilities, target privileged users and plan attacks. The resulting harm could extend to the security and availability of critical networks and systems,

placing at risk the information, systems and networks that public bodies are responsible for protecting.

Recommendation #10

Based on the position and best practices of security professionals across the country, Memorial University recommends stronger, more inclusive language in the ATIPPA to provide for the protection from disclosure of information respecting IT systems. This would be accomplished by having a separate section in ATIPPA dedicated to IT security protection.

[Recommendation 11: Access to Electronic Records \(s. 11 and 20\)](#)

Our Justification

Section 11 and section 20 of the *ATIPPA, 2015* address format of records.

Pursuant to ss. 11(2)(c), an applicant may indicate a preference for the form in which they prefer to access the record(s) sought. Accordingly, the ATIPP request application form invites applicants to indicate a preference.¹ Section 20 describes how access will be given to an ATIPP applicant. It states:

20. (1) Where the head of a public body informs an applicant under section 17 that access to a record or part of a record is granted, he or she shall

(a) give the applicant a copy of the record or part of it, where the applicant requested a copy and the record can reasonably be reproduced; or

(b) permit the applicant to examine the record or part of it, where the applicant requested to examine a record or where the record cannot be reasonably reproduced.

(2) Where the requested information is in electronic form in the custody or under the control of a public body, the head of the public body shall produce a record for the applicant where

(a) it can be produced using the normal computer hardware and software and technical expertise of the public body; and

(b) producing it would not interfere unreasonably with the operations of the public body.

(3) Where the requested information is information in electronic form that is, or forms part of, a dataset in the custody or under the control of a public body, the head of the public body shall produce the information for the applicant in an electronic form that is capable of re-use where

(a) it can be produced using the normal computer hardware and software and technical expertise of the public body;

(b) producing it would not interfere unreasonably with the operations of the public body; and

(c) it is reasonably practicable to do so.

(4) Where information that is, or forms part of, a dataset is produced, the head of the public body shall make it available for re-use in accordance with the terms of a licence that may be applicable to the dataset.

(5) Where a record exists, but not in the form requested by the applicant, the head of the public body may, in consultation with the applicant, create a record in the form requested where the head is of the opinion that it would be simpler or less costly for the public body to do so.

Through OIPC complaint investigations, the question of the right to access records in “native format” has been considered by the Information and Privacy Commissioner. Report A-2020-003 states:

[42] Section 11(2)(c) of ATIPPA, 2015 states that “A request shall indicate how and in what form the Complainant would prefer to access the record.” This section does not place an obligation on the public body to provide the records in the exact form requested. Section 20(2) states: (2) Where the requested information is in electronic form in the custody or under the control of a public body, the head of the public body shall produce a record for the Complainant where (a) it can be produced using the normal computer hardware and software and technical expertise of the public body; and (b) producing it would not interfere unreasonably with the operations of the public body.

[43] Section 20 also does not create an obligation to provide records in their native format, only in “electronic form”. Only section 20(3) is specific about the format indicating that:

(3) Where the requested information is information in electronic form that is, or forms part of, a dataset in the custody or under the control of a public body, the head of the public body shall produce the information for the Complainant in an electronic form that is capable of re-use where (a) it can be produced using the normal computer hardware and software and technical expertise of the public body; (b) producing it would not interfere unreasonably with the operations of the public body; and (c) it is reasonably practicable to do so.

[44] As the records in question here are not part of a dataset, this subsection does not apply. But even it does not speak of native format and contains the caveat if “it is reasonably practicable to do so”. There may be other very narrow circumstances in which the native format of a record is relevant, however nothing of that nature applies here.

Considerations regarding native formats:

Determining what, in fact, is the native format of a record can be challenging in itself. For example, if a student requests a record of their transcript, an official paper transcript can be printed or an electronic pdf file can be generated. While both transcript formats present the same information and both are deemed acceptable formats, one could argue that neither the paper nor pdf is the ‘native’ format of that record. In order to produce the transcript, a Memorial employee with appropriate system access credentials must log in to Memorial’s student information system (SIS) to generate the transcript. The employee runs a query of the SIS and SIS then presents the transcript to the SIS user and provides options to print or generate a pdf. Some may argue that the SIS and the applicable screens that display the data constitute the native format. But to go even further, the information used to generate a transcript is stored within a database in multiple database tables. It is the SIS that makes the request to

the database to retrieve the record details, essentially making the database the ‘native’ format for the transcript.

In this most basic example, the same can extend to most records in electronic format such as a receipt, invoice, birth certificate, release of grades, etc. The standard outputs are normally in user friendly formats such as paper or pdf, but systems are required to generate/display those records and databases to store the information in its most basic format.

These examples demonstrate that many records are produced in standard/usable formats to ensure the end user can access the record in a format-friendly and timely manner but the software applications and databases to produce those records can vary significantly with regards to technology and who has appropriate access privileges to access those systems/records within an organization.

The complexity of producing native formats is increased when a public body is responding to an access request. ATIPP coordinators coordinate the collection of records across a public body. Memorial University has hundreds of supported systems/applications in which records and data reside. That is why ATIPP coordinators must depend on employees across the public body to retrieve the applicable records responsive to an access request and provide them in formats that the ATIPP coordinators can access/review – normally standard desktop formats such as Excel, PowerPoint, PDF, Word, etc. It would not be reasonable, appropriate or cost effective to expect ATIPP coordinators to have all software and software application access privileges in place to access/review data and records in their native format across a public body.

If you extend the challenges of an ATIPP coordinator accessing native formats to an applicant requesting native formats, similar challenges arise (software requirements, software application access, etc.) but an access request also poses additional requirements of ensuring information is thoroughly reviewed in accordance with provisions of the *ATIPPA, 2015*. A line by line review is required to ensure that information subject to mandatory and discretionary exceptions to disclosure are identified. ATIPP Coordinators must print the records, sort them in chronological order, and scan them into pdf format so the records can be reviewed/redacted in the redaction software. The public body’s file number and page numbers are added to the responsive records to assist with management of ATIPP requests, and to assist the ATIPP coordinator, the Applicant, and the OIPC and Courts should a complaint or appeal ensue. Maintaining the native format through the redaction process is not possible.

As the above discussion shows, what exactly is meant by “native format” is not entirely clear and would differ depending on the systems and databases used to generate records. It is also worth noting that the Act entitles applicants to apply for access to **records** of a public body, which is the end user-friendly generated document (i.e. a transcript, a paystub, an email correspondence). The Act does not entitle an applicant access to the databases and software that generates the record. This would be extremely cumbersome for the public body and would not be within the spirit of what is intended in the Act. In most cases, the needs of an ATIPP applicant are met when provided with a paper or electronic PDF copy of the record(s). Releasing records in standardized usable formats adheres to the *Management of Information Act* and the *ATIPPA, 2015* as the format does not materially change the information that was originally created, sent or received. If the reason for a request for native formats is to conduct a forensic review of the record(s), for a law enforcement purpose for example, an access request under the *ATIPPA, 2015* is not the appropriate mechanism to support that type of in-depth review of records.

Recommendation #11

Memorial University asserts that the *ATIPPA, 2015* does not, and should not, afford a right of access to records in native format and recommends that no change be made to the legislation in that regard.

Recommendation 12: Privacy Impact Assessments (s. 72)

Our Justification

Memorial University's Procedure for Checking Privacy Compliance is attached to its Privacy policy. The Privacy policy and related procedures were adopted by the Board of Regents in 2008. It was updated in 2026, mainly to reflect certain outdated internal references.

The policy states:

8. To monitor compliance with the Privacy Policy, all projects involving personal information must be reviewed using the Privacy Compliance Checklist, in accordance with the [Procedure for Checking Privacy Compliance](#). This may determine that a Privacy Impact Assessment is required. This compliance requirement does NOT apply to research projects involving human participants which have received ethics approval from a duly-constituted research ethics board, including a research ethics body under the Health Research Ethics Authority Act.

The Procedure for Checking Privacy Compliance contains two steps:

- Privacy Compliance Checklist (equivalent to the "Preliminary Privacy Impact Assessment" used by the Government of Newfoundland and Labrador and referenced in s.72 of the *ATIPPA, 2015*)
- The University Privacy Officer may decide, on review of the Privacy Compliance Checklist, that a Privacy Impact Assessment is required but will first consult with the university's IAP Advisory Committee

The Procedure for Checking Privacy Compliance states:

Completed checklists must be submitted to the University Privacy Officer who will complete a review of the checklist results and may make recommendations to the responsible unit head regarding actions that may need to be taken to reduce any privacy risks identified and to ensure compliance with the legislation, the University's privacy policy, or related procedures. If Checklist results contain significant privacy risks, the University Privacy Officer will consult with the [IAP Advisory Committee](#).

...

Based on a review of [Privacy Compliance Checklist](#) results and other factors, the University Privacy Officer may determine that a full PIA is required. The University Privacy Officer will consult with the IAP Advisory Committee before rendering a decision regarding the need for a PIA. Although the University Privacy Officer may overrule the recommendation of the IAP Advisory Committee, he or she would do so only upon very careful consideration of the issues involved.

Privacy Compliance Checklists are required to be approved by the head of the relevant university unit. On review of the Privacy Compliance Checklist, the University Privacy Officer, in collaboration with the Director of Information Management and Protection, provides advice and recommendations to the unit to mitigate any privacy and security risks identified. Additionally, they work with the Office of General Counsel to review and negotiate agreements and contracts, if the project involves outsourcing, to ensure the university's obligations under the *ATIPPA, 2015* are met. Additionally, in accordance with the Procedure for Administering Privacy Measures within a Unit, all such contracts must have a Privacy Schedule appended.

Memorial has, in accordance with policy, conducted privacy compliance assessments of projects and programs since 2008.

Given its autonomy and unique environment, Memorial University is best placed to determine the form and type of privacy assessments needed for its diverse operations. We recommend accordingly that, in recognition of Memorial University's autonomy as recognized in the *Memorial University Act*, any amendment to s.72 along the lines recommended by the OIPC, add a section or paragraph that the university will submit preliminary privacy impact assessments and privacy impact assessments to the appropriate unit head and that Memorial University will determine the form and type of privacy assessments needed for its programs and services.

Recommendation #12

Memorial University recommends that section 72 be amended by adding a subsection as follows:

(5) Notwithstanding section 72(1) and (2), Memorial University shall, during the development of a program or service by Memorial University, submit to the Head:

- (a) A privacy impact assessment for the Head'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

Recommendation 13: Common or Integrated Programs

Our Justification

In connection with subsections 72(3) and (4), as a large and diverse higher education institution, the university's multiple campuses and units are engaged in numerous programs that, depending on how the term is defined, could be viewed as common or integrated programs. Subsections 72(3) and (4) state:

- (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.

To illustrate the scope and type of “common or integrated programs” at Memorial University, the examples below are categorized under Administrative and Academic Programming:

Administrative (with other NL public bodies)

1. Memorial University and College of the North Atlantic are partners in the annual CareerEco Job Fair in which students and graduates of both institutions and employers and other organizations can carry out recruitment, networking and promotion activities
2. Registrar’s Office – Department of Education in which personal information is shared by Education (EDU) with Memorial University for the purpose(s) of receiving and assessing high school transcript information for MUN applicants to determine admission and entrance scholarship eligibility; supporting student success initiatives; tracking participation rates at MUN (high school graduates from the provincial school system entering first semester studies immediately following graduation).
3. Faculty of Medicine and College of Physicians and Surgeons of Newfoundland and Labrador and Regional Health Authorities in connection with Practice Ready Assessments for eligible candidates to assess readiness to practice in Canada

Administrative (pursuant to legislation)

4. Memorial is required by legislation to share personal information pursuant to numerous legislative requirements, for example:
 - Registrar’s Office/Cashier’s Office/Scholarships Office and NL Student Aid in *Student Financial Assistance Act*
 - Registrar’s Office and Statistics Canada, pursuant to the *Statistics Act*
 - Human Resources and Health and Safety and WorkplaceNL (in connection with workers compensation; incident (injury) reports) pursuant to *NL Occupational Health and Safety Act* and Regulations
 - Support Enforcement Agency in connection with *Support Orders Enforcement Act*
 - Human Resources and NL’s Essential Workers Support Program
 - Facilities Management and Provincial Apprenticeship and Certification Board, concerning employees designated for certification, pursuant to the *Apprenticeship and Certification Act*
 - Canada Revenue Agency for tax purposes
 - College of Physicians and Surgeons pursuant to the *Medical Act, 2011*

- Department of Education and the Department of Immigration, Refugees and Citizenship Canada (IRCC) in connection with the Provincial Attestation Letter process, pursuant to the *Immigration and Refugee Protection Act (IRPA)*
- Health and Safety and Service NL, OHS Division, in connection with XED dose/scatter surveys and incident investigations, pursuant to the *Occupational Health and Safety Act* and *Regulation and the Nuclear Safety and Control Act*
- Health and Safety and Canadian Nuclear Safety Commission in connection with dose monitoring/registrations, pursuant to the *Nuclear Safety and Control Act*
- Health and Safety and Public Services and Procurement Canada, in connection with the *Human Pathogen and Toxin License Human Pathogens and Toxins Act (HPTA)* and the *Health of Animals Act (HAA)*
- Health and Safety and the Canadian Association Underwater Diving, in connection with scientific divers pursuant to the *NL Occupational Health and Safety Act* and CAUS standards
- Health and Safety in connection with controlled goods, pursuant to the *Canada Defense Productions Act* and the *Controlled Goods Act*

Academic Programming

5. Memorial's Faculty of Nursing, together with the Centre for Nursing Studies and the Western Regional School of Nursing, the latter two run by Newfoundland and Labrador Health Services (NLHS) offer collaborative nursing education. Students of all three schools are students of Memorial University and have a joint admission process.
 6. Information Sharing Agreement between Memorial University Faculty of Medicine and UPEI Faculty of Medicine
 7. With public bodies, government organizations (national and international), indigenous community sponsors and others that sponsor students
 8. With Government of Newfoundland and Labrador in connection with tuition vouchers program
 9. With Immigration, Refugees and Citizenship Canada for verification of international students
 10. Memorial University (Marine Institute) and College of the North Atlantic certificate of aquaculture joint program offering
 11. Memorial University (Marine Institute) and College of the North Atlantic for bridging into Memorial University programs
- A large number of Memorial's educational programs offer or require internships, field placements, residencies, practicums, etc.

12. All faculties on all campuses in which students do field placements, research and applied research internships, masters and doctoral internships, international youth internships, international indigenous internships, practicums, residencies, co-operative education, and clinical placements (these are examples, not a comprehensive list):

- Faculty of Medicine
- Faculty of Nursing
- School of Pharmacy
- School of Social Work
- Faculty of Engineering and Applied Science
- Faculty of Business Administration
- Faculty of Education
- School of Human Kinetics and Recreation
- Faculty of Science (e.g., Computer Science, Psychology)
- Faculty of Humanities and Social Sciences (e.g., Archaeology, Political Science, Sociology)
- Environmental Policy
- Diploma Programs (e.g., Police Studies, Performance and Communications Media, Geographic Information Sciences, Applied Ethics, Professional Writing)

Memorial University has agreements with many universities and organizations nationally and internationally. Indeed, it would not be a reach to say that every academic department and faculty has one or more MOUs with universities nationally and internationally, and even with other countries, to facilitate student exchanges.

Given the above, complying with 72(3) and 72(4) for agreements in academic programming and disclosures/sharing of information pursuant to requirements of provincial and federal legislation is impractical and would require unreasonable, extensive additional resources.

Recommendation #13

Memorial University recommends that s. 72 be amended by adding subsections as follows:

(6) Notwithstanding section 72(3) and (4), Memorial University shall notify the commissioner of a common or integrated program or service in connection with administrative matters, but not academic programming matters, at an early stage of developing the program or service.

(7) Notwithstanding section 72(3) and (4), the Head of Memorial University shall, where the Head receives a privacy impact assessment respecting a program or service described in subsection 6, for which disclosure of personal information may be permitted under paragraph 68(1)(u), the Head shall, during the development of the program or service, submit the privacy impact assessment to the commissioner for the commissioner's review and comment.

IV. GAPS IN THE LEGISLATION/OVERSIGHT CONCERNS

Several gaps in the legislation have become apparent since it was enacted over a decade ago in 2015. Memorial University offers the following suggestions and recommendations to ameliorate such gaps and oversights in the amendment of the *Act*.

Recommendation 14: A Deadline for Complying with the Commissioner's Recommendation(s)

Our Justification

The *ATIPPA, 2015* does not provide clear guidance on whether there is a deadline for complying with recommendations of the Commissioner. This should be clarified.

Under section 49(1), the public body has 10 business days to decide whether to comply with the recommendations of the Commissioner, and to provide notice to a person who receives a copy of the report (which includes a complainant). As noted above, the public body is considered to have agreed to the Commissioner's recommendations if notice is not provided within the 10 business days allotted. Subsections 51(1) and (2) permit the Commissioner to file an Order with the Court in respect of recommendations where the public body "agrees or is considered to have agreed under section 49 to comply with a recommendation of the commissioner referred to in subsection 50(1) in whole or in part but fails to do within 15 business days after receipt of the commissioner's recommendation" or where the public body fails to apply for a declaration under section 50.

The combined effect of these sections is that a public body has 10 business days to decide whether to accept recommendations, and a further 5 days to comply, or it may become subject to an Order in Court. Arguably, this imposes a 15-business-day deadline for compliance from the date it receives the recommendations. However, this requirement is not clearly delineated as a deadline, with the potential for applicants to receive additional disclosure after its deadline for a further appeal has passed.

Furthermore, if the Commissioner is empowered to review the duty to assist and/or grant orders in respect of the duty to assist, there should be a longer timeframe for compliance. In this respect, Memorial University notes that a 15-business-day deadline to conduct additional searches and release additional records is less than the 20-business-day deadline imposed for the original ATIPP Request, notwithstanding that there are additional consultations required within a public body in order to determine whether to accept recommendations and before any additional searches can be undertaken and new records processed.

Recommendation #14

Memorial University recommends to:

- Amend the legislation to clearly delineate that there is a statutory deadline for compliance with the Commissioner's recommendations.
- Extend the number of business days that a public body has to comply with the Commissioner's recommendation to at least 20 business days.

Recommendation 15: Application of the Rules of the Supreme Court, 1986 & the Appeal Process

Our Justification

Memorial University has been party to 26 actions arising under or related to the *ATIPPA, 2015* (all with the same self-represented applicant). In the course of these actions, Memorial University has been served with notices of inspection, interrogatories, interlocutory applications, requests for lists of documents, and requests for examination for discoveries and other similar procedures. This has increased the cost of complying with the legislation dramatically and, we believe, has also unnecessarily complicated proceedings that are meant to be expeditious. Clarification regarding the expedited nature of the *de novo* hearings under the *ATIPPA, 2015* is warranted. It will help to avoid an increased cost of compliance while ensuring timely access to information.

Section 57 of the *ATIPPA, 2015* provides that “the practice and procedure under the Rules of the Supreme Court, 1986 providing for an expedited trial, or such adaption of those rules as the court or judge considers appropriate in the circumstances, shall apply to the appeal.” At the same time, section 59 governs the conduct of the appeal. Section 59(1) states that the Court shall review the matter as a new matter “and may receive evidence by affidavit,” while subsection (3) contemplates that the Court may accept evidence in private. It states:

59. (1) The Trial Division shall review the decision, act or failure to act of the head of a public body that relates to a request for access to a record or correction of personal information under this Act as a new matter and may receive evidence by affidavit.

(2) The burden of proof in section 43 applies, with the necessary modifications, to an appeal.

(3) In exercising its powers to order production of documents for examination, the Trial Division shall take reasonable precautions, including where appropriate, receiving representations without notice to another person, conducting hearings in private and examining records in private, to avoid disclosure of

(a) any information or other material if the nature of the information or material could justify a refusal by a head of a public body to give access to a record or part of a record; or

(b) the existence of information, where the head of a public body is authorized to refuse to confirm or deny that the information exists under subsection 17 (2).

In practice, Memorial University has been obligated to file applications for sealing of records under section 59(3) where the Court is considering an appeal relating to redactions to records. Those applications have usually been contested in each of the *de novo* appeals.

The expedited trial rule states:

17A.09. (1) Notwithstanding that there may have been an application under rule 17.01, 17A.01, 40.03 or 40.04, the Court may, on application by any party where

(a) the claim is for a liquidated sum not exceeding \$15,000 excluding post-judgment interest and costs; or

(b) in any other case where action under this rule can be taken without injustice to any other party,

order the expedited trial of a proceeding or an issue in a proceeding, and may order that

(c) certain facts described in the order are not in dispute;

(d) pleadings be amended or closed within a fixed time;

(e) interlocutory applications be brought within a fixed time;

(f) procedures for examination for discovery be completed within a fixed time;

(g) examination for discovery be dispensed with or limited in nature and scope;

(h) other pre-trial applications or procedures be dispensed with or limited in nature and scope;

(i) evidence be adduced by affidavit;

(j) a party deliver a written summary of the proposed evidence of a witness within a fixed time;

(k) the evidence in chief of a witness be given in whole or in part by the production of a written statement;

(l) experts who have been retained by the parties meet, on a without prejudice basis, to determine those matters on which they agree and to identify those matters on which they do not agree;

(m) a pre-trial conference be held at a time and date to be fixed, at which any of the orders in this rule may be made; and

(n) a pre-trial conference be dispensed with and the proceeding be set down for trial on a trial list or, with the approval of the Chief Justice, set for trial on a particular date.

(2) On an application under rule 17A.09(1) the court may make such other order as is just for the purpose of expediting the trial of a proceeding.

(3) At the trial any facts ordered not to be in dispute shall be deemed to be established and the trial shall be conducted accordingly, unless the trial judge orders otherwise.

(4) A judge may, before or at trial, vary or set aside an order made under rule 17A.09(1) or (2).

Notably, Rule 17.09(1) contemplates an application to the Court for the purposes of proceeding on an expedited basis. Furthermore, it contemplates that the Court may order that evidence be provided by way of Affidavit under Rule 17.09(i) – a clear overlap with ss 59(1) of the *ATIPPA, 2015*.

Memorial University respectfully requests clarification of the process for a *de novo* hearing and the application of the *Rules of the Supreme Court, 1986*. In this respect, it asks that the legislation be amended to clarify that a *de novo* appeal shall proceed as an expedited trial on the basis of affidavit evidence, and that no further recourse to the *Rules of the Supreme Court, 1986* is permitted absent an

application to the Supreme Court pursuant to Rule 17A.09. It would further recommend that a first appearance date proceed by way of a case management meeting at which time the parties could discuss filing deadlines and applications that are contemplated under Rule 17A.09. Lastly, the ability to file a copy of the records in dispute with the Court under seal should not, in the context of access to information legislation, be contested or require an application. As a result, Memorial University recommends that the legislation require a public body to file an audit copy of the records under seal (an audit copy being a copy that delineates where redactions are applied but does not contain the redactions).

Recommendation #15

Memorial University recommends:

- That the legislation be amended to clarify that a de novo hearing shall proceed as an expedited hearing on the basis of affidavit evidence subject to further application to the Court for additional steps under Rule 17A.09.
- That the first appearance date shall proceed as a case management meeting at which the parties are to discuss any applications contemplated under Rule 17A.09 and scheduling deadlines.
- That further recourse to the *Rules of the Supreme Court, 1986* be prohibited absent an order of the Court under Rule 17A.09 (as contemplated by the application provision of the *Rules of the Supreme Court, 1986* in Rule 1.02).
- That all *ATIPPA, 2015* appeals be case managed, with the first date serving as the first case management meeting.
- That a public body be required to file an audit copy of the records under seal with the Court without the necessity of a sealing application.

APPENDICES

Appendix A: Volume of ATIPP requests and OIPC complaint investigations since 2016

Year	Total Number of ATIPP Requests Received	Total Number of OIPC Complaint Reviews
2016	105	4
2017	89	10
2018	110	7
2019	113	13
2020	105	9
2021	156	13
2022	184	8
2023	189	11
2024	264	27
2025	132	18
2026 (1 January – 5 October)	94	8