Memorial University
Supplemental Submission
to the
Access to Information and Protection of Privacy Act, 2015
Statutory Review Committee
December 18, 2020

Table of Contents

I. The Duty to Assist 3
II. Protection for IT Security Arrangements 6

This submission supplements Memorial University's submission on 27 November 2020. Memorial wishes to address the Duty to Assist and endorse points in the submission of the Government of Newfoundland and Labrador's (GNL) Office of the Chief Information Officer and elaborate on them in the university context.

I. The Duty to Assist

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 the Office of the Information and Privacy Commissioner form for filing an Access or Correction Complaint under section 42 invites complainants to select "I am requesting that the Commissioner bring to the attention of the head of the above noted public body a failure to fulfill the duty to assist applicants" (available at https://www.oipc.nl.ca/pdfs/AccessComplaintorApplicationRelatedtoCost.pdf).

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, he has 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.*[1]

At best, a recommendation to conduct a further search for records is a Soft Recommendation falling 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.*

As noted (on pages 26-27) in Memorial University's main submission, an appeal to the Court following a Commissioner's Report under section 54 is limited to the issues of "access to the record" and correction of personal information (Hard Recommendations). A Commissioner's Recommendation on the duty to assist is not appealable.

The provision regarding direct appeals to the Court contains broader language. It states:

> *52. (1) Where an applicant has made a request to a public body for access to a record or correction of personal information and has not filed a complaint with the commissioner under section 42, the applicant may appeal the decision, act or failure to act of the head of the public body that relates to the request directly to the Trial Division.*

The Court's jurisdiction to issue a decision regarding the duty to assist, inclusive of searches, has not been judicially considered. Section 60 governs the Court's order making power on an appeal. It states:

> *60. (1) On hearing an appeal the Trial Division may*
> - *(a) where it determines that the head of the public body is authorized to refuse access to a record under this Part and, where applicable, it has not been clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception, dismiss the appeal;*

[1] Office of the Information and Privacy Commissioner of Newfoundland and Labrador, *Memorial University (Re)*, Report A-2019-018 (August 15, 2019), available online: https://www.oipc.nl.ca/pdfs/A-2019-018.pdf .

(b) where it determines that the head of the public body is required to refuse access to a record under this Part, dismiss the appeal; or

(c) where it determines that the head is not authorized or required to refuse access to all or part of a record under this Part,

(i) order the head of the public body to give the applicant access to all or part of the record, and

(ii) make an order that the court considers appropriate.

(2) Where the Trial Division finds that a record or part of a record falls within an exception to access under this Act and, where applicable, it has not been clearly demonstrated that the public interest in disclosure of the information outweighs the reason for the exception, the court shall not order the head to give the applicant access to that record or part of it, regardless of whether the exception requires or merely authorizes the head to refuse access.

(3) Where the Trial Division finds that to do so would be in accordance with this Act or the regulations, it may order that personal information be corrected and the manner in which it is to be corrected.

Reading the legislation as a whole, Memorial University is of the view that the duty to assist is not reviewable on appeal, neither following an OIPC Report (as a "Soft Recommendation) nor on a direct appeal to Court. If, however, the duty to assist is appealable on a direct appeal under section 52, that can encourage applicants to by-pass the OIPC complaint process in favour of the more costly Court process, thereby increasing the cost of compliance for public bodies. If the duty to assist is not appealable at all (either following an OIPC Report or by going directly to Court), this raises the question of whether the duty to assist is instead reviewable by way of judicial review. This possibility may result in bifurcation of review proceedings whereby redactions are reviewable on an appeal *de novo,* but the duty to assist is reviewable by way of judicial review.

A further issue arises when a public body decides to comply with a Soft Recommendation regarding the duty to assist. For instance, if the Commissioner issues a Soft Recommendation to conduct an additional search for records, what occurs if additional records are located, and the applicant again takes issue with the redactions applied or the searches conducted?

Similarly, if the duty to assist is appealable to Court under section 52, and the Court orders a further and better search for records, what occurs if the requester again takes issue with the searches and/or the redactions applied to new records located as a result of that Court Order?

Such a scenario ought to be addressed, bearing in mind that the *ATIPPA, 2015* is intended to provide timely access to records and bearing in mind, too, the costs of compliance for a public body and the necessity of clearly establishing when a public body's obligations, and its duty to assist a requester, ends. Memorial has had experience with a scenario in which the OIPC recommends a further search and some further records are located. The applicant then takes issue with the new search conducted and the redactions applied, which then follows with a new complaint, and ultimately when the applicant is not satisfied with the complaint response, another appeal to court. Then we have a situation in which there are two court applications arising from the same set of circumstances. Memorial cautions against a

circular complaint process in favour of finality and timely access.

Recommendation 11
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

II. Protection for IT Security Arrangements

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 University endorses the submission on this point (on pages 3-4) by the Government of Newfoundland and Labrador's Office of the Chief Information Officer.

We would add the following points about IT security in a university environment:

1. Universities, by the nature of their business, have a significantly large threat surface. Memorial's user community and relationships are worldwide in nature.

2. Memorial University has one of the largest IT environments in the province and has connectivity to the provincial government, regional health authorities, national and international networks, other universities, major private organizations, etc. The impact of a major security breach could be far reaching and involve non-Memorial entities.

3. Canadian federal cybersecurity organizations, including the Canadian Security Establishment (CSE), have frequently issued warnings directly to universities, including directly to Memorial University, indicating that hackers are actively attempting to infiltrate Canadian universities and other public/private organizations.

Security related information is being used as a weapon in cyber-attacks:

1. The Canadian Centre for Cyber Security has a short but effective video on the risks associated with administrative privileges: https://cyber.gc.ca/en/administrative-privileges

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. Privilege is power. Cyber criminals are known to breach vulnerabilities in networks/systems and use elevated privileges (their own or stolen) to penetrate and breach large organizations. These threats are real and have already happened at numerous Canadian universities including York University and University of Calgary. "Attackers frequently target systems administrators and other professionals in order to gain the passwords and credentials to break into other systems." https://portswigger.net/daily-swig/a-guide-to-spear-phishing-how-to-protect-against-targeted-attacks

4. The FBI recently published a warning about spear phishing and noted in particular "incidents of spear phishing - targeted phishing attacks - are increasingly taking aim at employees with administrative rights and access to critical systems." https://blog.knowbe4.com/bid/313516/FBI-Warns-of-Spear-Phishing-Attacks

Memorial University is a frequent target of cyber-attacks. Some examples and statistics for context:

1. Memorial's network is under constant assault by both foreign and domestic entities, including state actors, attempting to gain access to our network.

2. Brute force attacks are attempted on Memorial's network roughly every couple of weeks.

3. In April 2020, Memorial's Office of the Chief Information Officer observed an increase in traffic that, over a period of days, resulted in a total accumulation of hundreds of millions of attempts to connect to the campus that was sourced from China, Russia, the Netherlands, and other overseas entities. Billions of connection attempts sourced from overseas have been blocked at the campus firewall.

4. Memorial deployed additional security tools to further protect the network based on new activity since COVID-19. These security tools use vendor designed proprietary detection methods based on industry standards to identify and drop malicious traffic. More than 90 million malicious connections were dropped within the first 30 days of deployment.

5. An average week of Memorial firewall statistics show hundreds of millions of rejected hits. Many days since COVID-19 have shown elevated levels of attack traffic in the range of 1 billion every couple of hours.

6. Attacks are becoming more sophisticated in nature and harder to detect by end users and by tools and technology. Memorial regularly receives phishing, spear-phishing and spoofing emails against its user population. Popular targets often align with published names on websites, public lists and forums. These targets include Memorial's president, vice-presidents, deans and other senior leaders.

7. On average during the summer of 2020, the university received approximately 950,000 - 1 million emails every 24 hours, of which 80-85% are threat messages and are blocked. Email volumes can often exceed 3-7 million over a 24 hour period during elevated attack periods.

How ATIPPA can be used as a weapon against public bodies:

Disclosing information piecemeal in response to ATIPP requests, for example software versions here, patch levels there, and names of system/network administrators, enables attackers to carefully accumulate information to undertake attacks that could cause serious and far-reaching harm to the overall security and availability of critical networks and systems and as a result put at risk the information that public bodies are responsible for protecting.

Recommendation 15

Based on the position and best practices of security professionals across the country, including the Government of Newfoundland and Labrador Office of the Chief Information Officer, 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.