Memorial University
Supplemental Submission
to the
Access to Information and Protection of Privacy Act, 2015
Statutory Review Committee
February 12, 2021

Table of Contents

This submission supplements Memorial University's submission on 27 November 2020. Memorial wishes to provide information on cyber threats, providing records in electronic format under s.20, and the recommendation by the Office of the Information and Privacy Commissioner that the requirements under s.72 be extended to other public bodies.

I. Cyber Threats

Section 31(1)(l) is a discretionary exception to disclosure that permits a public body to withhold information that would reveal computer 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 has one of the largest and most complex IT environments in the province. On a daily basis, university IT staff respond and react to security threats against its environment.

To complement Memorial's supplemental submission dated December 18, 2020 (pages 6-8: Protection for IT Security Arrangements), Memorial University is providing additional detail in support of Recommendation 13 listed below.

1. Information posted on Memorial University web servers is crawled by major search engines, like Google, on a weekly basis. This information is made available as search results on those platforms. In addition to major search engines, university web sites are frequently scanned for content/intelligence for malicious purposes. These searches scan for content such as system configurations, patch levels, application versions, operating systems and developer/administrator names.

2. Attacks are becoming more sophisticated and harder to detect by end users, tools and technologies. Memorial University regularly receives phishing emails targeting its user population. These emails often impersonate legitimate services or businesses with the intention of tricking users into providing personal information or user credentials for Memorial University's systems. Information is powerful in the hands of malicious users. Security information in the public domain can be used to create fake sites that look realistic or used to target specific individuals within an organization. At Memorial University, popular targets for phishing emails are the president, vice-presidents, deans and directors.

3. Every 24 hours, Memorial's email security devices reject over 80-85% of inbound emails directed at our user population. This represents approximately 1 million rejected requests per day, many of which represent phishing emails targeting Memorial users. During heavy email periods, upwards of 3-7 million emails are blocked in a single 24 hour period.

4. Perimeter firewalls are one tool in a multi-layered system that help protect Memorial University's IT infrastructure. The perimeter firewall rejects ***billions*** of requests on a monthly basis. Providing security related information in response to ATIPP requests puts security information in the public domain and increases the chance this information can be used to breach systems.

5. Records containing details about IT infrastructure may include information identifying the location of critical infrastructure and the security controls in place to protect it. Examples of sensitive information include credentials, IP addresses, hostnames, other system identifiers, vendor and technology names, versions, network configurations, security assessments and diagrams, among others. When malicious users are in possession of this information, there is an increased probability of attack and increased likelihood the attack will be successful.

6. When responding to ATIPP requests, subject matter experts, such as IT experts, may need to be engaged to identify sensitive security information that may fall outside traditional disclosure exceptions. An example could be as simple as an interpretation of a website address to determine if any sensitive information is embedded in the URL link. While traditional disclosure exceptions may be well understood when responding to ATIPP requests, other security risks may not be well understood or may have changed from a risk perspective since last discussed. It is important to have strong, clear language in ATIPPA to protect this type of information from disclosure.

As referenced in our initial supplemental submission, Memorial University also endorses a similar position put forth by the Government of Newfoundland and Labrador's Office of the Chief Information Officer's submission related to the importance of protecting information related to the security of IT systems (on pages 3-4). Memorial reiterates Recommendation 12 (incorrectly numbered as 15) in our Supplemental Submission dated 18 December 2020.

II. Access to Electronic Records (s.11 and 20)

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*

[1] See for example https://www.mun.ca/iap/access/ and https://apps.gov.nl.ca/atipp/

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[2] 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.*

[2] A-2020-003, available at https://www.oipc.nl.ca/pdfs/A-2020-003.pdf

> *[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 13
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.

III. Privacy Impact Assessments (s.72)

Memorial University's Procedure for Checking Privacy Compliance[3] is attached to its Privacy policy[4]. The Privacy policy and related procedures were adopted by the Board of Regents in 2008.

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*)

[3] Available at https://www.mun.ca/policy/browse/procedures/view.php?procedure=103
[4] Available at https://www.mun.ca/policy/browse/policies/view.php?policy=228

- 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[5], all such contracts must have a Privacy Schedule[6] 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.

[5] Available at https://www.mun.ca/policy/browse/procedures/view.php?procedure=486

[6] Two Privacy Schedules are available at: Resources | Information Access and Privacy | Memorial University of Newfoundland (mun.ca) . One is for contracts where data are stored in Canada and one for data stored outside Canada.

Recommendation 14

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

Common or Integrated Programs

In connection with subsections72(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*
    - 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 Eastern Regional Health Authority's Centre for Nursing Studies and the Western Regional Health Authority's Western Regional School of Nursing offer collaborative nursing education. Students of all three schools are students of Memorial University and have a joint admission process.
6. With public bodies, government organizations (national and international), indigenous community sponsors and others that sponsor students
7. With Government of Newfoundland and Labrador in connection with tuition vouchers program
8. With Immigration, Refugees and Citizenship Canada for verification of international students
9. Memorial University (Marine Institute) and College of the North Atlantic certificate of aquaculture joint program offering

10. 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.

11. 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):
    a. Faculty of Medicine
    b. Faculty of Nursing
    c. School of Pharmacy
    d. School of Social Work
    e. Faculty of Engineering
    f. Faculty of Business
    g. Faculty of Education
    h. School of Human Kinetics and Recreation
    i. Faculty of Science (e.g., Computer Science, Psychology)
    j. Faculty of Humanities and Social Sciences (e.g., Archaeology, Political Science, Sociology)
    k. Environmental Policy
    l. Diploma Programs (e.g., Police Studies, Performance and Communications Media, Geographic Information Sciences, Applied Ethics, Professional Writing)

12. 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 15

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.