ABOVE BOARD

A quarterly newsletter published by the Office of the Information and Privacy Commissioner

Volume 14, Issue 4 October 2022

Contact Information

Office of the Information and Privacy Commissioner

3rd Floor, 2 Canada Drive
Sir Brian Dunfield Building
P.O. Box 13004, Station A
St. John's, NL A1B 3V8

Telephone:

709-729-6309

Fax:

709-729-6500

Toll Free in Newfoundland and Labrador:

1-877-729-6309

Email:

commissioner@oipc.nl.ca

www.oipc.nl.ca

This Issue:

Right to Know Week 2022

The Office of the Information and Privacy Commissioner (OIPC) invited the public to "Know Your Rights" during the annual Right to Know (RTK) Week, which was held September 26th to October 2nd. RTK Week in Canada evolved from International Right to Know Day, September 28th, which has been marked around the world since 2002.

RTK Week recognizes the importance of the right of access to information held by government and other public bodies. Access to information means government transparency and accountability, and provides citizens with knowledge to address public issues, scrutinize government and become active participants in the democratic process.

In an effort to ensure all individuals can access these rights, the OIPC, with the assistance of sign language interpreter Sheila Keats, developed a video for deaf, hearing-impaired, and visually-impaired individuals. In this video, Commissioner Michael Harvey provides audio explaining individual rights under the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*), which is simultaneously interpreted into American Sign Language, as well as captioned for a wide variety of audiences.

Part of the mandate of the OIPC is public education. By providing accessible videos and easily digestible information, the OIPC is helping to ensure all community members "know their rights". To view this video, please visit www.oipc.nl.ca/events/right-to-know-week.

Privacy Tort of Intrusion Upon Seclusion Recognized for the First Time in Newfoundland and Labrador

In August 2022, a decision from the Newfoundland and Labrador Supreme Court officially recognized the privacy tort of "intrusion upon seclusion" for the first time in this province.

Intrusion upon seclusion is a relatively new tort by legal standards. It was first recognized by the Court in Ontario in 2012 in *Jones vs. Tsige*, establishing that, "One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the invasion would be highly offensive to a reasonable person."

A tort is a wrongful act or an infringement of a right which leads to loss or harm for an individual. There are statutory torts, where civil liability is established by a provincial statute, and there are common law torts, where civil liability is established by judge-made decisions known as judicial precedent.

The elements required to make out the tort are:

(a) the defendant's conduct must be intentional;
(b) the defendant must have invaded, without lawful justification, the plaintiff's private affairs; and
(c) a reasonable person would regard the invasion as highly offensive causing distress, humiliation and anguish.

Although the tort has existed for ten years, it has only been formally recognized in a few provinces, including Ontario and Newfoundland and Labrador This is because intrusion upon seclusion remains limited and requires criteria to clearly and obviously meet the elements.

In *Power v. Mount Pearl (City)*, 2022 NLSC 129, Justice MacDonald made two determinations relating to the intervenor, Mr. Steve Kent. In the decision, Justice MacDonald determined that the City of Mount Pearl infringed upon Mr. Kent's privacy rights, and in doing so, MacDonald stated at para. 26:

> *[...] Therefore, I find that Newfoundland and Labrador has a common law tort for intrusion upon seclusion. Furthermore, I find that this right coexists with rights created under the Privacy Act*.

As a result of the infringement on Mr. Kent's privacy rights, MacDonald determined that the evidence obtained through the breach would not be part of the Record in the broader case of *Power.*

This development in privacy law in the province has significant consequences for future civil privacy cases. In addition to the province's *Privacy Act* legislation, which permits civil actions in situations where a breach of the *Privacy Act* has occurred specifically, the recognition of intrusion upon seclusion adds an additional layer of civil remedy to privacy violations.

Note: This issue is currently under appeal.

Joint Resolution of the Federal, Provincial and Territorial Privacy Commissioners – Securing Public Trust in Digital Healthcare

Newfoundland and Labrador Information and Privacy Commissioner Michael Harvey was proud to host the annual meeting of the Federal, Provincial and Territorial Information and Privacy Commissioners and Ombudspersons in St. John's on September 19-21, 2022. This was the first face-to-face meeting of Commissioners since 2019 and the meeting involved presentations from several experts and valuable discussions on topics of mutual interest.

Commissioner Harvey is proud to announce, as an outcome of the meeting, the issuance of a Joint Resolution on Securing Public Trust in Digital Healthcare, endorsed by all of Canada's Privacy Commissioners and Ombudspersons.

In recent years new technologies have become available that involve both novel ways of providing care, including virtual care, as well as modern methods of collecting, storing and using personal health information. This trend has meant that the health sector is a more data rich environment than it has ever been before. The COVID-19 pandemic has accelerated this trend both to expand the reach of clinical care through virtual means and to use technology to find efficiencies in a highly burdened health care system.

Protecting sensitive personal health information is critical to maintaining Canadians' trust in the health system. If properly designed, selected and implemented, modern technologies provide the potential for greater privacy protection. The health sector has been notorious for using outdated and vulnerable technologies, such as faxes and unencrypted email, threatening to erode the public's confidence that their personal health information is secure. Adoption of modern digital communications systems can improve privacy and security and increase the public's trust in their health care system.

Commissioners therefore made a series of recommendations to governments and health care providers to modernize their health information systems and legislative frameworks so that they meet the privacy principles that are enshrined in health information statutes across the country as well as meeting the high standard of protection against breaches – both intentional and unintentional – that Canadians have a right to expect. For their own part, Commissioners are committed to collaboration with stakeholders in the sector, and engaging with the public, about technological change in digital health communications.

Upcoming Training Opportunities

Did you know that both the OIPC and the ATIPP Office offer training on access and privacy topics? You can contact the OIPC to request a customized session on *ATIPPA, 2015*, *PHIA* or broader presentations on access or privacy topics by emailing commissioner@oipc.nl.ca or by calling 729-6309.

Upcoming sessions offered by the ATIPP Office include:

- Communities of Practice: Communities of Practice are held every few months and focus on a specific topic relevant to Access to Information and Privacy. Any ATIPP Coordinator, Backup Coordinator, or privacy analyst is welcome to attend.

- Access to Information Training for ATIPP Coordinators: This training is designed for new ATIPP Coordinators or Backup Coordinators and can also be taken as a refresher course. It takes place over two days, from 9:30-12:30 each day. This training covers how to use the various exceptions, the steps to process a request, resources available and various challenges.
- Privacy Training for ATIPP Coordinators: This training is designed for new ATIPP Coordinators or Backup Coordinators and can also be taken as a refresher course. It takes place over two days, from 9:30-12:30 each day. The training focuses on the Privacy side of the *Act*, including legislation and best practices around the collection, use and disclosure of personal information, privacy breaches and privacy impact assessments.
- Cabinet Confidences Training: This training covers the complexities of processing ATIPP Requests that involve cabinet records. This training takes 2 hours.
- Municipal Access to Information and Protection of Privacy Training for Municipal ATIPP Coordinators: This virtual training is designed for both new or existing Municipal ATIPP Coordinators who want to learn about the *Act* or want a refresher course. It takes place over two days, from 9 -12 each day. This training covers how to use the various exceptions, the steps to process a request, best practices around the collection, use and disclosure of personal information, privacy breaches, privacy impact assessments, resources available and various challenges. This training can be conducted with groups or individually depending on the needs of the Coordinator.

If you are interested in attending any of these sessions, please register by emailing ATIPPoffice@gov.nl.ca; please include the training session(s) you want to attend in the subject line. While the Communities of Practice has a set date, other training will be scheduled based on interest and the availability of participants.

Processing an Access Request: Consultations

Public bodies have obligations under *ATIPPA, 2015* to process access requests within the statutory timeframe. While public bodies have developed their own systems for processing requests, we have received inquiries about consultations with other public bodies.

There is nothing in *ATIPPA, 2015* that requires consultations; there is also nothing that prohibits consultations. In fact, consultations can be a valuable part of the access process. For example, if a Coordinator is uncertain about the applicability of an exception, the ability to consult with a subject matter expert, even one in another public body, can be valuable in clarifying the matter.

Coordinators should remember that the *Act* contains tools that may be more appropriate than consultation; for example, would a transfer be more appropriate for the request?

Section 13(1) 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.*

OIPC notes that the public body that received the request is ultimately accountable for compliance with legislation, unless the request was transferred. Further, in a complaint investigation situation, it is the public body that responded to the request that will have to support its decisions.

Public bodies seeking consultations should provide the records involved as early as possible in the process. It is possible that not all the responsive records for a request require consultation and public bodies should provide only the records at issue for consultation.

If your public body receives a request for consultation, you are encouraged to promptly action this request. When another public body is faced with missing a legislative deadline because a consultation is incomplete, it may decide to proceed without input from your public body, based on its own understanding of the record and applicable exceptions.

ATIPPA, 2015 Privacy Breach Statistics July 1 – September 30, 2022

During the third quarter of 2022 (July 1 to September 30, 2022), the OIPC received 33 privacy breach reports from 20 public bodies under *ATIPPA, 2015*. Almost half the breaches involved email (21), with an additional six involving mailouts, two in-person and four breaches attributed to other causes.

Given the high number of email breaches, we have a few steps that employees can take to reduce or prevent email-related breaches.

- Turn off Outlook's Auto-Complete address feature under File > Options > Mail > Send Messages; this can prevent you from inadvertently sending an email to a recipient with a similar name.
- Use your address book to populate To, Cc and Bcc fields.
- When sending an email, using a previous email from the intended recipient and replying – rather than composing an entirely new message – can avoid potential errors in entering the address or selecting the correct recipient. This can be particularly useful when corresponding with someone outside of your organization: wait until they have successfully sent you an email, and you can confirm its authenticity, before replying with personal information.
- Delay the delivery of emails through Outlook's Rules & Alerts. An extra two minutes spent in the Outbox might be enough to realize a mistake and catch an error in an email before it is sent.

If any public body would like the OIPC to deliver training regarding privacy breaches, or any other topic relating to access or privacy, please contact our Office to arrange a time.

The OIPC has issued a Tip Sheet on avoiding inadvertent privacy breaches.