ABOVE BOARD

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

Volume 13, Issue 3 July 2021

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:

Final Report of ATIPPA Statutory Review Committee Released

On June 9th, the final report of the *Access to Information and Protection of Privacy Act* (*ATIPPA*) Statutory Review Committee 2020, chaired by retired Supreme Court Justice David B. Orsborn, was published. The final report is available online here.

ATIPPA, 2015 requires that a comprehensive review of the provisions and operation of the Act be undertaken every five years. The *ATIPPA* Statutory Review 2020 Committee was established by the Government of Newfoundland and Labrador to conduct an independent statutory review of *ATIPPA, 2015*. The Committee examined the operation of the Act and made recommendations intended to ensure that the objectives of the Act are realized.

"The Honourable David Orsborn clearly did a very thorough job and we appreciate his hard, thoughtful and diligent work," says Commissioner Harvey. "We will need to examine it with the same care that he wrote it. That said, now as much as at any time in our history, government transparency is critical so we will be doing our review as quickly as possible and we encourage the Government to also treat the matter with urgency."

Commissioner Harvey also recognizes the efforts of those who made submissions to the Committee and encourages public bodies to review the final report. While it remains for the Government to decide what amendments, if any, will be introduced into the House of Assembly, proposed amendments that will likely be of particular interest to ATIPP Coordinators include:

- Changes to the fee structure, with an increase of "free" hours to 35 and the ability to charge for "identifying, locating, retrieving, reviewing, severing, redacting" for requests that take over 35 hours
- Changes to the definition of "business day" to exclude "other days on which a public body is not open for business"
- Changes to timelines for responses, with pauses for clarifications, verification of the identity of the applicant and applications to the OIPC for approval to disregard a request
- Changes to the authorities of the public body, such as the ability to disregard a request if the clarification or verification of identity is not done within 30 business days; to disregard a request where records or information are available through existing procedures; to self-extend by 10 business days in certain circumstances; and to extend the time for a response with the consent of the applicant
- Expansion of the requirement to complete a privacy impact assessment to all public bodies and the introduction of automated decision system and algorithmic impact assessment
- Requirements for public bodies to develop information practices, policies and procedures for handling personal information
- Introduction of a process to declare an applicant vexatious

This is a not a comprehensive summary of all recommended amendments, which are extensive. OIPC continues to review the report and may have additional content in upcoming newsletters.

Investigator's Conference – Administrative Fairness

OIPC NL staff were fortunate to virtually participate in a national Investigator's conference with our federal, provincial and territorial counterparts, held April 26th – 27th. Our colleagues across the country developed sessions on administrative fairness, dealing with difficult behaviours, increasing efficiency/reducing backlog, and approaches to early case resolution. We'd like to thank the joint efforts of our federal, provincial and territorial colleagues for organizing this event, with special thanks to the Office of the Saskatchewan Information and Privacy Commissioner for hosting.

One thought-provoking presentation was on administrative fairness. Administrative fairness has three components:

- Fair process, which requires participation by all parties, as well as integrity and impartiality. It provides an opportunity for all parties to be heard and ensures that adequate information about the process is provided. Decisions should be free from personal interest or prejudice and communicated fairly, including relevant evidence, legislation and policy that form the basis for the conclusion.
- Fair decision, which is a decision that is equitable, just and lawful. It is extremely difficult to determine a fair decision when no or limited information is provided.
- Fair service, which is people-centered, accessible, accountable and one that involves continuous improvement. As part of fair service, it is important to accommodate diverse service users and demonstrate courtesy and respect. When possible, it is important to use clear and plain language.

The presentation noted that the work done by oversight offices and public bodies all have a role to play in ensuring fairness. A great resource called Fairness by Design: An Administrative Fairness

Self-Assessment Guide was developed by the Offices of the Ombudsman in Saskatchewan, Manitoba, Nova Scotia and Yukon and of the Ombudsperson in British Columbia. The Office of the Citizen's Representative for Newfoundland and Labrador highlighted this tool in its September 2019 newsletter.

We encourage public bodies to assess and ensure administrative fairness is built into policies and processes when dealing with the public.

Federal, Provincial and Territorial Privacy Commissioners Release Joint Statements

Privacy and COVID-19 Vaccine Passports

The Federal, Provincial and Territorial Privacy Commissioners released a Joint Statement on Privacy and COVID-19 Vaccine Passports on May 19th; the Canadian Council of Parliamentary Ombudsman released a document called Fairness Principles for Public Service Providers Regarding the Use of Vaccine Certification on May 26th.

Both documents provide considerations for the development or implementation of such a method to obtain goods or services. Some overlapping considerations include the importance of reviewing programs once developed, of complying with existing legal requirements such as privacy and human rights law, of ensuring independent oversight and of developing programs that ensure proportionality of privacy risks and program benefits.

The Commissioner and the Citizens' Representative also consulted the Newfoundland and Labrador Human Rights Commission, which observed that any organization implementing a vaccine passport should remember that discrimination/harassment is prohibited against people with disabilities and people perceived to have disabilities. The duty to accommodate people still applies.

Privacy and Access Rights During an Emergency

On June 2nd, a Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners regarding privacy and access rights during an emergency was released.

The resolution adopted 11 access to information and privacy principles and recognizes the impact that the global pandemic has had on rights to privacy and access to information. It calls on government to use the lessons learned during the pandemic to improve those rights.

"While the pandemic has resulted in a global slowdown in processing access to information requests, that impact was mitigated in Newfoundland and Labrador through strong access to information legislation and the hard work of public employees," notes Commissioner Harvey. "There were some delays, however, and we encourage public bodies to utilize technology and improved records management to minimize any future impacts. Government transparency during a crisis is critical, and access to information is an important part of openness and accountability."

Commissioner Harvey encourages governments, both provincial and municipal, and other public bodies to review the Joint resolution and consider taking appropriate action.

Surveillance: Access and Privacy Issues

The issue of surveillance continues to be in the news and the subject of both access and privacy reports from our Office, as well as our counterparts across the country.

Facial Recognition

At a national level, facial recognition has been a topic of interest. The Privacy Commissioner of Canada appeared before the Standing Committee on Access to information, Privacy and Ethics (ETHI) on Facial Recognition Technology. The Federal Privacy Commissioner also participated in a joint investigation, along with the Commission d'accès à l'information du Québec, the Office of the Information and Privacy Commissioner for British Columbia and the Office of the Information and Privacy Commissioner of Alberta, into a company called Clearview AI.

Clearview AI created a database containing over 3 billion images, including those of Canadians and children, using public sources, such as news media, public social media, and many other open sources. The company's technology allowed law enforcement and commercial organizations to match photographs of unknown people against the company's databank of images for investigation purposes. Commissioners found that this creates the risk of significant harm to individuals, the vast majority of whom have never been and will never be implicated in a crime.

The investigation concluded that the New-York-based technology company violated federal and provincial privacy laws when it collected highly sensitive biometric information without the knowledge or consent of individuals. Although Clearview AI has stopped offering its software to Canadian clients, the company has refused to comply with the investigation's two other recommendations: to delete previously collected data and to stop collecting images of Canadian residents.

The Privacy Commissioner of Canada also investigated the use of Clearview AI by the Royal Canadian Mounted Police (RCMP). In a news release, the Commissioner released his findings that the RCMP violated the *Privacy Act* when it used Clearview AI. The Commissioner concluded that the RCMP could not collect personal information from a third party if that third party had collected the information unlawfully; the RCMP did not agree with this conclusion. In the same release, the Commissioner issued draft guidance to assist police in ensuring any use of facial recognition technology complies with the law, minimizes privacy risks and respects privacy rights.

OIPC NL contacted the Royal Newfoundland Constabulary (RNC) about this matter and the RNC confirmed that it had never used the services of Clearview AI or any other facial recognition service, and further had no plans to do so.

Another joint investigation saw the Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Columbia and the Office of the Information and Privacy Commissioner of Alberta examine Cadillac Fairview, a real estate company behind some of Canada's most popular shopping centres. Cadillac Fairview embedded cameras inside digital information kiosks at 12 shopping malls to collect millions of images and used facial recognition technology to convert those images into biometric numerical representations of individual faces, about five million images in total. During the testing phase, the cameras also captured audio.

Although the technology could be used to identify individual shoppers, Cadillac Fairview said it used it to assess foot traffic and track shoppers' ages and genders. The company also argued shoppers

were made aware of the activity through decals it placed on shopping mall entry doors that warned cameras were being used for "safety and security" and included the web address for Cadillac Fairview's privacy policy. The Commissioners concluded that this did not meet the standard for meaningful consent. A further issue was the storage of the five million images; they were stored in a centralized database by a third-party company on a decommissioned server, with no identified purpose and with no justification.

The investigation found the technology was used in five provinces, including Alberta, British Columbia, Manitoba, Ontario and Quebec. The company suspended its use of cameras in 2018 and has announced that the data collected has been deleted.

Both investigations lead to calls for changes to existing privacy laws, pushing for updated laws that reflect new and emerging technologies and allow for fines/higher fines.

Provincial Reports

OIPC NL has released three reports that examined the issue of surveillance and access to surveillance footage.

Both Report A-2021-014 and Report A-2021-009 examined access to surveillance footage. In the first instance, a request for video surveillance footage was refused based on section 40 of the *Access to Information and Protection of Privacy Act, 2015* (disclosure harmful to personal privacy). Additionally, the public body contended that it did not possess the necessary equipment or software to de-identify the footage. The Commissioner concluded that the public body must acquire or source the capacity to de-identify persons recorded by its video surveillance systems and recommended that some video recordings be disclosed after they are de-identified.

The Report stated, in part:

> *The means to de-identify surveillance video records is an essential part of any CCTV system operated by a public body, and if a public body implements CCTV capability it also needs redaction software, as it is an essential tool required to process requests for access to records. If you have paper records, you need a black marker; if you have electronic records (including video surveillance records), you need electronic redaction software.*

In Report A-2021-009, an access request was made for body-worn camera and vehicle camera footage. The public body refused access under a number of sections; it is the discussion on section 40 (disclosure harmful to personal privacy) that is most pertinent for other public bodies. Part of the public body's argument was that the personal information, specifically the image, actions and voice, of an employee are captured on the video. At paragraph 27, the report concluded that this, "...would not be considered an unreasonable invasion of privacy if released, as section 40(2)(f) of ATIPPA, 2015 would apply allowing disclosure of information about a third party's position, functions or remuneration as an officer, employee or member of a public body."

While the Report concluded that the footage should continue to be withheld from disclosure to protect the privacy of others featured in the video, it states at paragraph 29,

> *[29] In this access to information request, the applicant was not one of the individuals captured on the video. If that had been the case, there would have been*

a right of access by that person to their personal information under section 40(2)(a) of ATIPPA, 2015, subject to other individuals' personal information being protected.

Report P-2021-002 examined the use of body-worn cameras (BWCs) by a municipality. The BWC program was initiated for municipal enforcement officers and the Commissioner launched an own-motion investigation after the program began collecting personal information. The Report contains a detailed discussion of Municipal Enforcement Officers and their authority for collecting personal information, and OIPC encourages municipalities with enforcement divisions to review it. Subsequent to the issuance of that Report, the Town filed an application in Court to seek a declaration that it need not follow our recommendations. That matter is ongoing at this time.

ATIPPA, 2015 Privacy Breach Statistics April 1 – June 30, 2021

During the second quarter of 2021 (April 1 – June 30, 2021), the OIPC received 45 privacy breach reports from 20 public bodies under *ATIPPA, 2015*; 24 of the breaches involved email. Public bodies are reminded that tips on avoiding breaches, including email breaches, can be found here.

Two intentional breaches were reported during this period; both involved abuse of authorized access. For the second quarter in a row, the Royal Newfoundland Constabulary reported a breach involving a staff member looking up their own information in the MRD system. Workplace NL had a staff member look up the information of a family member; while the family member contacted the staff member and requested that this action be taken, it is a violation of appropriate system use. As such, both incidents meet the definition of an intentional privacy breach because it was an unauthorized use.

TIPS and TRICKS

Corresponding with OIPC

Did you know? While OIPC accepts complaint forms and other correspondence by mail and fax, we also accept (and largely prefer) using email. Our general email is commissioner@oipc.nl.ca.

Reminder: Response to Reports MUST include Right to Appeal

Public bodies are reminded that final responses to OIPC Reports MUST inform the complainant of the right to appeal. Section 49 discusses the response of the public body and 49(3)(a) establishes the requirement that the written notice include the right of the applicant or third party to appeal to the Trial Division under section 54 and of the time limit for an appeal. OIPC NL has noticed that some responses are missing this critical piece in their responses and have had to ask for a modified letter at times. This is time consuming for both parties and, for public bodies that send responses signed by the head or other senior staff, it can be embarrassing for the ATIPP Coordinator to get a signature on a second letter. Furthermore, the appeal timelines protect the rights of applicants, which is crucial to the entire process.