ABOVE BOARD

A QUARTERLY NEWSLETTER PUBLISHED BY THE OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

VOLUME II, ISSUE I FEBRUARY 2019

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
Tel: (709) 729-6309
Fax: (709) 729-6500
Toll Free in Newfoundland and Labrador: 1-877-729-6309
E-mail: commissioner@oipc.nl.ca
www.oipc.nl.ca

"The Commissioner's role is to facilitate the effort of a requestor to seek access to information […] and is effectively an ombudsman or liaison between the citizen and government in attempting to resolve the request by mediation or otherwise if documents or information known to be existing are being withheld in whole or in part for various reasons"

Justice Harrington, NL CA, NL (Information and Privacy Commissioner) v. NL (Attorney General)

OIPC REMINDERS AND UPDATES

Upcoming OIPC Workshop

The OIPC will be hosting a Workshop on Monday, April 1st to further discuss the development of Privacy Management Programs (PMPs).

In March, 2018, we held a Workshop to discuss the Privacy Management Program framework and our expectations in relation to the same. We now expect that discussions regarding PMPs will have commenced within public bodies and, to that end, the upcoming Workshop will discuss the importance and role of policies and procedures in instituting a PMP and creating a privacy culture. We will look at necessary policy topics and essential discussion points.

Please note, we will be offering this Workshop twice on April 1st in order to accommodate the level of interest in this session. The timing of the sessions are as follows:

- Morning Workshop: 9:30a.m.—11:30a.m.
- Afternoon Workshop: 1:30p.m.—3:30p.m.

The Workshop will be held in Conference Room A in the West Block of the Confederation building.

If you and/or any other individuals in your organization would like to attend, please RSVP to Stacey Pratt (staceypratt@oipc.nl.ca) and **be certain to indicate which Workshop you will be attending**.

Training Reminder

Did your staff have *ATIPPA, 2015* training in 2018?
If not, consider contacting our Office to arrange for training in 2019.
Also, consider whether you would like training about any specific access or privacy topic.

PRIVACY MANAGEMENT PROGRAMS: OIPC EXPECTATIONS

The OIPC has been fielding many questions about our expectations with a Privacy Management Program (PMP). What is reasonable will vary based on such considerations as the volume of personal information held, as well as the sensitivity of the information.

Some public bodies will find it fairly easy to develop a PMP for a variety of reasons. Take, for example, a public body that does not hold much personal information, the personal information it does hold is not sensitive and the public body enjoys a mature privacy culture. There is probably a PMP already in place, either formally or informally, so the gap analysis may reveal that much of the work required for a PMP is already complete. Compare this with a public body that holds massive databases of personal information, much of it sensitive, with limited awareness of privacy. There will be much more work to be done to develop and document a PMP.

Any public body that has personal information has legislative obligations under the *ATIPPA, 2015*. Part of those obligations is to ensure reasonable safeguards are in place to protect personal information in its custody and control. One assumes that, the more sensitive the information, the greater the safeguards. This includes ensuring that appropriate privacy resources are in place to identify and address privacy concerns associated with the personal information. The public body that holds large quantities of sensitive personal information should have more privacy resources in place than the public body with little personal information.

When conducting the gap analysis, it is possible that a number of gaps will be identified, requiring the public body to prioritize them. This Office would expect that gaps that represent high risks are addressed early in the PMP process, while low risk gaps may take longer. If a public body identifies a number of high risk areas, it may need to dedicate additional resources to address them in a timely fashion.

The OIPC expectations will also consider the passage of time. These guidelines were released in March 2018. We do not expect public bodies to be in compliance immediately. What we do expect is evidence of efforts towards compliance. We expect public bodies to take the time to look at the guidance, understand how it impacts the organization, and take action to be in compliance. Our oversight approach allows more flexibility at the outset in circumstances where public bodies face legitimate challenges and can document that best efforts are underway to bring the public body into compliance.

While what is deemed reasonable may vary, what is certain is that the further out we are from the issue date of the PMP guidance document, the more this Office expects. Public bodies and custodians that are subject of a privacy complaint or who submit a breach report can expect to be asked about the privacy tools it uses, such as PMPs and PIAs, on a go forward basis. Public bodies that cannot demonstrate any effort to develop a PMP will be hard pressed to demonstrate compliance with the *ATIPPA, 2015*.

(continued on next page...)

PRIVACY MANAGEMENT PROGRAMS: OIPC EXPECTATIONS (continued)

We have also received calls regarding a template for a PMP. The PMP guidance document identifies the expectations of this Office and each public body needs to determine what this will look like for them. As this will vary, this Office has no current plans to develop a template; there is no one template that will suit every public body. That being said, various support tools are under development. Stay tuned....

R v JARVIS: ESTABLISHING A REASONABLE EXPECTATION OF PRIVACY

The Supreme Court of Canada recently gave its decision in *R v Jarvis* a case involving a high school English teacher who videotaped female students using a hidden camera. The students did not know of nor consent to the recordings. The recordings were mainly of the students upper bodies and faces.

In convicting the teacher of voyeurism, the Court provided a list of circumstances that should be used in determining whether an individual has a reasonable expectation of privacy from observation or recording. While the list is not exhaustive, its nine elements provide a solid direction for the courts in determining if individuals are entitled to expect privacy.

1) **The location of the person during the observation or recording.** Whether the location is one which excludes all or permits only certain others.
2) **Type of intrusion.** Observation or recording. Recordings are accepted as being more privacy intrusive than observations.
3) **Awareness of or consent to potential observation or recording.** Surreptitious observations or recordings may tend to be more privacy intrusive.
4) **How was observation or recording carried out.** Was the intrusion a singular incident or repeated. How long did it last? Was the recording kept or destroyed? There are many factors to be considered here.
5) **The subject matter or content of the observation or recording**. Who was involved? What were they doing? What specifically was viewed?
6) **Any rules, regulations or policies that governed the observation or recording in question**.
7) **The relationship between the parties.** Was there a relationship of trust or authority?
8) **The purpose of the observation or recording**.
9) **The personal attributes of the person who was observed or recorded.** Children or other vulnerable persons may have a heightened expectation of privacy.

While it is an interesting decision, public bodies must be mindful that the decision in *Jarvis* speaks specifically to the charge of voyeurism and is given in relation to the actions of an individual, not a public body. Legislation such as the *ATIPPA, 2015* and *PHIA* place additional obligations and expectations on public bodies when collecting personal information via video surveillance.

ANONYMITY FOLLOWING A COMMISSIONER'S REPORT

Anonymity When Responding to a Commissioner's Report

In relation to the recommendations contained in a Commissioner's Report, the *Act* requires a public body to provide written notice of its decision to the Commissioner and all persons who received a copy of the Commissioner's Report. The notice must be in writing. In instances where more than one individual received a copy of the Report, public bodies must be cautious in copying all parties on one notification letter. In these instances, public bodies must not disclose personal information in the copy line. The copied parties should simply be referred to as "Applicant", "Third Party", etc.

Anonymity in Court Proceedings

Where a public body chooses to seek a declaration not to comply with a recommendation of the Commissioner, a copy of the application for a declaration must be served on the Commissioner, the minister of the Department of Justice and Public Safety, and all parties who were sent a copy of the Commissioner's Report. While the Complainant must be served with a copy of the application for a declaration, the Complainant is not a Respondent to the application and should not be named in the application. While the court may later require that the identity of the Complainant be disclosed – and the Complainant should not be assured of anonymity at this stage for this reason – unless this occurs, the identity of the Complainant should not be provided in the court documents.

Furthermore, as with a public body's response to a Commissioner's Report, if more than one party is receiving the same copy of the declaration, public bodies must not disclose personal information in the copy line.

Our Guidance Document on Anonymity of Applicants will be updated shortly to reflect these positions.

OPENGOV WEEK

March 11-17, 2019 is Open Government Week.

Canada has joined the Open Government Partnership (OGP) in celebrating transparency, accountability, and participation in government.

This year's theme in Canada is inclusion; focusing on increasing the number and diversity of citizens participating in government.

For more information on what Canada's doing for Open Government Week, please visit our website. To learn more about the global Open Government week, please visit OGP's website.

INTERACTING WITH APPLICANTS

As an ATIPP Coordinator you will be called upon to interact with access to information applicants. Section 13 of the *ATIPPA, 2015* mandates that public bodies 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." When an access request is received, the Coordinator should reach out to the applicant to ensure that they fully understand the nature of what the applicant is requesting and seek any necessary clarity. In cases where there are other issues between the public body and the applicant, these discussions may be uncomfortable or seemingly futile but efforts should still be made. Additionally, before discussing the request with the applicant, the Coordinator should have discussions with relevant staff members to understand what responsive records the public body has or may have in order to have a meaningful discussion with the applicant and manage expectations. These discussions with the applicant may result in a file transfer or perhaps serve as evidence if the public body wishes to seek a time extension or a disregard. Be certain to keep records of all conversations with the applicant.

Following receipt of a Commissioner's Report, the public body is required to give notice of its decision in relation to the Commissioner's recommendations to all parties who received a copy of the Report. This will include the applicant. This notification is essential as it starts the applicant's appeal period should they wish to appeal the public body's decision. Coordinators should reach out to the applicant to advise that the decision has been sent and to ensure it has been received.

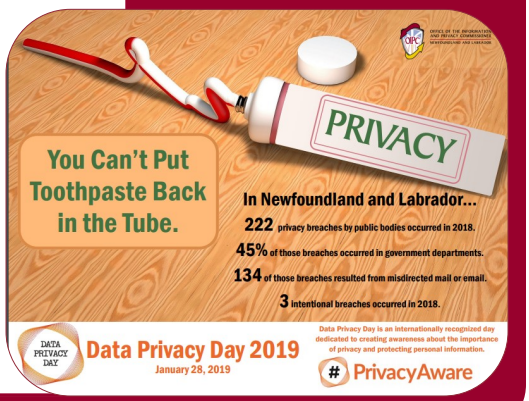
Interacting with Individuals Affected by Privacy Breaches

Finally, in relation to privacy breaches, public bodies must be mindful that should notification of the breach be provided to affected individuals, that notification must include reference to the right of the individual to file a complaint with the OIPC. It should also provide the contact information for the OIPC. The OIPC breach notification form requires that you advise our Office if this reference was not included in the notification letter.

Data Privacy Day (DPD) was January 28, 2019.

The OIPC created two posters in celebration of the event which are available on our website.

While DPD has passed, the message on the posters are still applicable and may be posted in your organization.



ATIPPA, 2015 PRIVACY BREACH STATISTICS Oct. 1 - Dec. 31, 2018

During this reporting period (October 1 — December 31, 2018), the OIPC received 48 privacy breach reports from 24 public bodies under the *ATIPPA, 2015*. While the number of breaches has decreased from the previous reporting period, the number of public bodies with reported breaches has increased.

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

Summary by Public Body	
City of Corner Brook	1
City of Mount Pearl	2
City of St. John's	2
College of the North Atlantic	2
Dept. of Advanced Education, Skills and Labour	4
Dept. of Children, Seniors and Social Development	4
Dept. of Education and Early Childhood Development	1
Dept. of Justice and Public Safety	1
Dept. of Municipal Affairs and Environment	1
Dept. of Service NL	4
Dept. of Transportation and Works	1
Eastern Health	2
Human Resource Secretariat	1
Human Rights Commission	2
Memorial University	1
Newfoundland and Labrador English School District	1
Newfoundland and Labrador Housing Corporation	4
Newfoundland and Labrador Legal Aid Commission	6
Office of the Chief Information Officer	2
Office of the Public Trustee	1
Town of Torbay	1
Western Integrated Health Authority	1
Workplace Health, Safety and Compensation Review Division	1
Workplace NL	2

Summary by Type	
Email	20
Fax	5
In Person	4
Mail Out	12
Other	7

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