



ABOVE BOARD

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

VOLUME 05, ISSUE 02

DECEMBER, 2015

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
Email:

commissioner@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 Projects
- * Privacy Impact Assessments
- * Notification of Individuals Following a Privacy Breach
- * Privacy Breach Statistics
- * Revised Municipalities Guide
- * Recent NL Court of Appeal Decision
- * Section 39 OIPC Guidance Document

OIPC Projects

Activities This Quarter

Privacy review of automated tax clearance certificate program

Social media and privacy presentation to Provincial Student Leadership Conference

Privacy presentation to Municipalities NL

Privacy presentation to Workplace NL

Hosted CCTV workshop

Privacy presentation to WHSCC Review Division

NL Housing privacy breach training

ATIPP Community of Practice presentations on section 39 and Privacy Breach

Activities Planned For Next Quarter

Section 39 (Disclosure harmful to third party business interests) guidance document

Brochures for citizens regarding privacy rights and access rights

Article about privacy to appear in Institute of Municipal Assessors newsletter

Section 30 (legal advice) guidance document

Section 27 (cabinet confidences) guidance document

Privacy impact assessment content guidance document

Details of OIPC audit program to be released

PRIVACY IMPACT ASSESSMENTS

A privacy impact assessment (PIA) identifies and evaluates the potential effects on privacy of a project, initiative, or proposed system or scheme.

The *Access to Information and Protection of Privacy Act, 2015 (ATIPPA, 2015)* defines a PIA in section 2(w) as *an assessment that is conducted by a public body as defined under subparagraph (x)(i) to determine if a current or proposed program or service meets or will meet the requirements of Part III of this Act.*

In general, it is best practice to conduct a preliminary PIA (PPIA) prior to starting a full PIA; the information contained in the PPIA may indicate that a full PIA report is needed.

Recent changes to the *ATIPPA, 2015* require departments and the executive branch of government to complete a PIA or PPIA during the development of a program or service. Further, if the PIA involves a common or integrated program or service, the minister must notify the OIPC regarding this program at an early stage of development. Once a PIA in relation to a common or integrated program or service is developed, it must be submitted to the OIPC for the Commissioner's review and comment. As the *ATIPPA, 2015* does not define a common or integrated program or service, the OIPC adopted a definition similar to the one in Schedule 1 of British Columbia's *Freedom of Information and Protection of Privacy Act*:

common or integrated program or service means a program or service that

a) provides one or more services through
(i) a public body and one or more other public bodies or agencies working collaboratively, or
(ii) one public body working on behalf of one or more other public bodies or agencies

Further details are located in section 72 of the *ATIPPA, 2015* and in our [PIA guidance document](#).

While not all public bodies are required to conduct PPIAs and PIAs, it is good practice and would be something the OIPC would likely ask to see during an audit of a program or service, as PIAs are an excellent tool to identify and mitigate privacy risks. In addition, while it is not required that the OIPC review all PIAs, this Office would welcome the opportunity to review and provide comments on any PIA that is conducted by a public body.

Further, section 95 of the *ATIPPA, 2015* establishes the general powers and duties of the Commissioner. This Office has the authority to conduct investigations to ensure compliance with the *ATIPPA, 2015* and to monitor and audit practices and procedures employed in carrying out responsibilities and duties under the *ATIPPA, 2015*. Where appropriate, the PIA process would be part of such investigations and audits, as it should help to demonstrate how a public body planned or intended to address identified risks.

NOTIFICATION OF INDIVIDUALS FOLLOWING A PRIVACY BREACH

When a privacy breach occurs, public bodies must notify the individual whose privacy has been breached as a result of their personal information being stolen, lost, disposed of contrary to law or disclosed to or accessed by an unauthorized person – section 64(4).

However, where a public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information they do not have to notify the individual – section 64(7).

"Significant harm" is defined in Section 64(8) as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

The factors that are relevant to determining whether a breach creates a risk of significant harm to an individual under subsection (7) are set out in subsection (9) including the sensitivity of the personal information; and the probability that the personal information has been, is being, or will be misused.

Therefore the decision of whether to notify the individual must be carefully considered by the public body. The OIPC recommends that when considering whether to notify an individual or not, you place yourself in the shoes of the individual and consider whether under the specific circumstance the affected person may consider the breach one that might cause significant harm. Also, public bodies should

consider the ability of the individual to take specific steps to mitigate or avoid any such harm.

When notification of the breach is sent, public bodies should include the date and a description of the breach, exactly what personal information was impacted, the steps planned to prevent future breaches, steps the individual can take to mitigate the risk and contact information for an individual within the public body and the OIPC (including their right to file a complaint).

Section 64(5) states that notwithstanding a circumstance where, under subsection (7), notification of an individual by the head of a public body is not required, the Commissioner may recommend that the head of the public body, at the first reasonable opportunity, notify the individual who is the subject of the information.

Section 64(4) outlines the obligation that a public body must report all breaches, whether minor or major, to the OIPC.

We caution against a trend we have noticed of some public bodies who are choosing not to notify individuals. We strongly recommend that you consider each notification or lack thereof on a case by case basis. It is our view that if there is any uncertainty about whether to notify someone about a breach of their personal information, it is much better to err on the side of caution and notify.

PRIVACY BREACH STATISTICS SECOND QUARTER

The OIPC received 61 privacy breach reports from 21 public bodies. This is up from the 44 reports from 16 public bodies received in the [first quarter](#) of mandatory breach reporting.

Since the last quarter's statistics were reported, the OIPC has provided training to some public bodies on what constitutes a privacy breach in an effort to support and promote compliance with the *ATIPPA, 2015* privacy provisions and to ensure that all public bodies understand the requirement to forward all privacy breach reports to this Office.

Privacy breach reports to the Commissioner allow the OIPC to advise public bodies about the breach response process and discuss ways to avoid similar breaches. This information is also used by the Commissioner to decide whether to initiate an investigation or an audit, and also to identify specific issues or public bodies for privacy training.

While many reported privacy breaches are relatively minor in nature, trends and patterns in breach reports can reveal more serious systemic issues over time. For that reason, the Commissioner continues to emphasize that all privacy breaches must be reported regardless of how minor they may appear at first.

If you want the OIPC to deliver training regarding privacy breaches, or any other topic, contact our Office to arrange a time.

Summary by Public Body

College of the North Atlantic	7
Advanced Education and Skills	13
Child, Youth and Family Services	7
Environment and Conservation	1
Justice and Public Safety	3
Municipal and Intergovernmental Affairs	1
Natural Resources	1
Transportation and Works	1
Eastern Health	1
Forestry and Agrifoods Agency	1
House of Assembly	1
Human Resource Secretariat	3
Human Rights Commission	1
Memorial University of Newfoundland	1
Newfoundland and Labrador English School District	1
Newfoundland and Labrador Housing Corporation	5
Office of the Public Trustee	1
Service NL	4
Western Health	1
Workplace NL	3
Workplace Health, Safety and Compensation Review Division	4

Summary by Breach Type

E-mail	22
Fax	2
In Person	8
Mail Out	22
Other	6
Telephone	1

REVISED MUNICIPALITIES GUIDE

On November 3, 2015, the OPE through its ATIPP Office, released an updated Access to Information and Protection of Privacy [Guide for Municipalities](#). The guide was updated in consultation with the Municipal Working Group. This group included representation from the OIPC, the Department of Municipal and Intergovernmental Affairs, Municipalities NL, the ATIPP Office, municipalities in the Province and the Implementation Team created to carry out all of the recommendations of the Wells Committee.

This revised Guide for Municipalities has been developed as a resource to support municipalities as they navigate the new *ATIPPA, 2015* and carry out their day to day activities, such as preparing minutes, discussing information with councilors and responding to requests for information from citizens. A further update to this guide will be provided when a standard for disclosure for municipal governance is enacted in the *Municipalities Act, 1999*, as recommended by the Wells Committee.

The guide contains a discussion on disclosure of “public documents”, which are those documents that a municipality is required to make available to the public in accordance with section 215 of the *Municipalities Act, 1999*. These public documents are available to the public during normal business hours and a person does not need to submit a formal access request under *ATIPPA, 2015* in order to view these documents. The guide also contains a section on how a municipality should deal with personal information in public documents. The Guide for Municipalities has an informative section dealing with privacy issues which discusses such matters as collecting, using, accessing and disclosing personal information; sharing personal information with members of council; the use of personal information on social media and dealing with privacy breaches (including a Privacy Breach Protocol).

The guide provides essential information on dealing with access to information requests. The points covered include: receiving and processing access requests, the duty to assist applicants, the exceptions to disclosure, the new public interest override in section 9 of *ATIPPA, 2015* and new time limits for responding to an access request. There is also a section dealing with access requests for specific types of information such as public documents, minutes of meetings, recordings of meetings, records relating to privileged meetings, property documents, the name of an access to information applicant, complaints made to a municipality, and information related to staff of a municipality.

As can be seen, the updated Guide for Municipalities is an important resource for municipalities containing valuable information for maintaining compliance with the provisions of the new *ATIPPA, 2015*. It is not a document to be consulted only when there has been an access request to a municipality or there has been a privacy breach. Rather, it is an essential tool to be consulted and reviewed regularly by the municipality’s access and privacy coordinator, by the staff of the municipality and by members of council, in order to ensure good municipal governance in relation to access to information and protection of privacy.

Recent Decision of the NL Court of Appeal (2015 NLCA 52)

In *Corporate Express Canada Inc. v. Memorial University of Newfoundland* the request was for information about the cost of office supplies Memorial purchased from Staples under the tender contract and also supplies purchased outside the contract. The court stated:

One prospective bidder's loss of exclusive knowledge of MUN's contract and non-contract usage of office supplies in a previous time period, without more, does not translate to a risk of harm considerably above a mere possibility, or a real risk of financial loss. More specifically, disclosure of MUN's usage information simply puts prospective bidders on a more equal footing. This is how it should be, for it ultimately makes MUN, as a public institution, more accountable in its expenditure of public monies.

Section 39 Exception

Section 39 is an exception to an applicant's right of access which is intended to protect from disclosure any business information of a third party which would harm that party's business interests.

It is a mandatory exception to the right of access, which means that if the information meets all the requirements of the exception, the public body must refuse to disclose it to an applicant.

In order to apply this exception, the public body must meet all parts of the three-part test. The information must:

- 1) reveal trade secrets or commercial, financial, labour relations, scientific or technical information of a third party;
- 2) be supplied in confidence; and
- 3) there must be a reasonable expectation of one of the harms listed in 39 (1)(c).

The OIPC is developing a guidance piece to assist public bodies in applying this exception which will be available soon on [our website](#).

Quick Tip

Notifying the Third Party only needs to happen when there is some evidence to support the exception but not enough to discharge the burden of proof required.

This only occurs when the public body intends to release the information in spite of the possible application of the exception.

If the exception clearly does not apply – no notice is required.

If the exception clearly does apply and the public body has enough evidence to support the application of the exception – no notice is required.