ABOVE BOARD

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

VOLUME 05, ISSUE 01 SEPTEMBER, 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
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

Training from the OIPC

The *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) has been in force now for over 3 months. You must have questions! Well, we have answers.

The mandate of the Office of the Information and Privacy Commissioner (OIPC) was increased by the new *Act.* Under *ATIPPA, 2015* this Office is empowered to create an educational program for the public and to inform public bodies of their responsibilities and duties under this *Act* - section 95(2)(b).

In accordance with this, we have produced six guidance documents for public bodies, which can be found at http://www.oipc.nl.ca/atippaguidancedocuments.htm. We will be adding to these regularly, with guidance for third party claims coming soon.

Further, the OIPC will be conducting workshops during the fall of 2015 and we would like to know what topics you (the Access and Privacy Coordinators) would like us to address. Please share with us any questions you have or ideas for workshops by emailing us at commissioner@oipc.nl.ca so we can craft an education program that fits your needs.

The exact timing and length of these workshops will be announced soon. We are aware of how busy you are and hope to make these workshops the best possible use of your time.

We are also developing a guidance document for members of the public so they can better understand the access process. We hope this will be a useful tool for you as you assist members of the public with the *ATIPPA, 2015*.

ATIPPA, 2015 is now a reality, let's work together to make it work as it was intended, to streamline the access to information process for everyone involved and to ensure that we protect the privacy of the citizens we serve.

The Danger of Unencrypted Flash Drives

On Tuesday, June 23, 2015, the OIPC was notified by Eastern Health (EH) that an unencrypted flash drive containing the personal information of 9000 Eastern Health employees, including the social insurance numbers of 3300 EH employees, had been lost or, possibly, stolen from EH's Human Resources office.

The information had been placed on the flash drive by a student employee who was documenting the hard copies of all employee files held by EH to assist with EH's transition to a fully electronic system. The student indicated that the drive was last seen on Wednesday, June 17, 2015 and on Friday, June 19, 2015 the flash drive could not be located.

Pursuant to section 73(3) of the *ATIPPA, 2015*, on June 24, 2015, the Commissioner commenced an investigation on his own motion with respect to this apparent contravention of the *Act*.

In due course, the OIPC received 35 privacy complaints from affected individuals. An investigation of all matters related to the lost flash drive continued until the OIPC was notified on Wednesday, August 5, 2015 that the missing flash drive had been located. The flash drive was found by an EH employee in a file folder within the secure facility in which it belonged and from which it had supposedly gone missing.

As a result of this incident, EH made a commitment to implement the following changes to prevent similar situations from arising in the future:

1. no longer using Social Insurance Numbers as employee identifiers;
2. requiring employees to answer a series of security questions to verify their identity when requesting information;
3. requesting the return of all non-encrypted USB drives and the destruction of same;
4. upgrading EH's antivirus platform so that any non-encrypted flash drives which remain in use will automatically be encrypted upon the use of those drives for storage purposes;
5. implementing new device controls which will force all other forms of mobile devices through a lock-down or encryption process; and,
6. creating a new policy regarding the issuance, control and use of mobile devices.

Many of these changes have already been implemented and the remainder will be implemented by the end of September, 2015. The Commissioner accepted that these changes were in line with the recommendations which would have been made had the USB drive not been located and had EH not proactively initiated these changes. Consequently, the Commissioner decided not to proceed with a review. The Commissioner has, however, chosen to follow up with EH in three months to verify that all the changes have been implemented.

Third Party Notification

One of the changes that *ATIPPA, 2015* brought was the removal of the notification to Third Parties when the public body was considering whether to give access. Now, under section 19 (1) the public body only notifies the Third Party when it "intends to grant access to a record" which they have "reason to believe contains information that might be excepted from disclosure".

This has created the need for some new procedural changes both at the OIPC during the complaint process and for the public body. For the public body, it is important to note that section 19(8) requires the public body to "advise the applicant as to the status of a complaint filed". Therefore, when a third party makes a complaint to the OIPC, we will not be engaging with the original access to information applicant during our process, unless we feel it would be beneficial to the investigation. Therefore, if we issue a report recommending release of the information following a third party complaint, the public body has an obligation to notify the original access to information applicant of our report, their decision in response to the report, and if they or the third party has filed an appeal.

The procedure is more complicated when the public body decides to rely on section 39 (disclosure harmful to the business interests of a third party) themselves. In that case the public body bears the burden of proof under section 43(1), however the public body is sometimes not in the best position to defend its use of that exception. Often the third party has industry-specific information that can assist in discharging the burden of proof.

If the public body has not already engaged with the third party (as they are no longer required to notify the third party if they do not intend to release), their case to the OIPC may be lacking in critical evidence. It is our recommendation that when a public body receives notice of a complaint, that they consult with the third party to prepare their representation to this Office.

The Commissioner has discretion under section 96(1) to seek representations from any person during an investigation. If this Office feels the public body will not meet the burden of proof, and therefore that the recommendation will be for release, we have the option to seek a representation from the third party directly. This is not ideal as this could be the first notice of a possible release of their information and it must be done within the required timeframe for the investigation. Extra time for them to prepare a response is not available within the tight timelines of the *ATIPPA, 2015*.

The best course of action for public bodies who have claimed section 39 is to consult with the third party in the early stages of a complaint, even if they feel the section's application is clear. The only other option, where the public body feels they may not meet the burden of proof, is to provide notice of an intention to give access to the third party under section 19 (1). If the third party does not object, the information is released. If the third party objects, they may complain to this Office, thereby shifting the burden of proof to the third party, who may have the relevant evidence and information.

Privacy Breaches

Chairperson Clyde Wells wrote in the *ATIPPA* Review 2014 Report that:

> *"The need for more effective protection of personal information is recognized internationally."*

Wells addressed privacy breach reporting by stating:

> *"Since relatively few data breaches from public bodies are documented, the optimal requirement would be to report all breaches to the Commissioner, who could recommend any necessary follow up, notification of the affected parties if that has not already been done, preventative measures for the future, and so on."*

Wells opined on the following benefits to reporting privacy breaches:

> *"Data breach reporting better informs and protects individuals who may be the victims. It also sensitizes the public body and its personnel to the importance of data security at all times."*

A privacy breach is the result of an unauthorized access to, or collection, use or disclosure of personal information. It includes but is not limited to: a fax sent to the wrong recipient, an email sent to the incorrect user, unintentionally putting correspondence meant for one person in an envelope addressed to another or snooping by an employee.

ATIPPA, 2015 makes it mandatory for all public bodies to report all privacy breaches to the OIPC. A dedicated email address (breachreport@oipc.nl.ca), reporting form (http://www.oipc.nl.ca/pdfs/PrivacyBreachIncidentReportForm.pdf) and guidelines (http://www.oipc.nl.ca/pdfs/BreachNotificationGuidelines.pdf) have all been prepared to assist public bodies in complying with this legislative requirement.

Since the enactment of *ATIPPA, 2015* on June 1, 2015 the OIPC has noticed that more public bodies are reporting privacy breaches. However, we are concerned that not all public bodies are meeting their statutory obligation. If you believe you may have had a privacy breach and have not yet reported it, please get in touch with the OIPC.

From March 17 to August 31 the OIPC received 85 breach notifications from a total of 46 public bodies. Of note, there are 6 core government departments and most municipalities that have not yet reported a breach. We ask all public bodies to review the legislation and our guidance document to determine if they should be reporting breaches to this Office.

If you have any questions regarding privacy breaches such as what is a privacy breach, is this incident a breach, how do I report a breach, what do I do once a breach has been identified or other questions, please contact the OIPC. We are here to help.

CCTV Guidelines and Upcoming Survey of Surveillance Camera Usage

The Office of the Information and Privacy Commissioner has updated its Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador. The OIPC first published CCTV guidelines almost a decade ago, however advances in technology and the introduction of *ATIPPA, 2015* necessitated the creation of a new and improved set of guidelines. The new guidelines can be found at http://www.oipc.nl.ca/pdfs/GuidelinesForVideoSurveillance.pdf and are applicable to all public bodies under *ATIPPA, 2015*, including municipalities.

If your public body is currently operating/using a surveillance system, or if you are considering the installation/use of CCTV in the future, the OIPC strongly recommends that you examine the guidelines and understand the specific implications that CCTV can have from both an access and privacy perspective.

The OIPC will be conducting a survey of public bodies this fall to determine the extent of the usage of CCTV in this Province and to identify ways that we can assist public bodies in complying with the guidelines. We ask that you help us to help you by completing this survey when you receive it this fall. If you have any questions on these guidelines or if you wish to discuss the access and privacy consequences of a CCTV system, please contact the OIPC.

Highlights from the CCTV Guidelines

(for complete list see link above)

Public bodies should draft policies and procedures that outline the roles and responsibilities of individuals or groups involved in the collection of personal information by CCTV. These should include, for example:

* documentation of the decision, including a detailed rationale and purpose for the surveillance;
* limits on the collection of personal information to that which is necessary to achieve the stated purpose, including a description of the kind of information collected through the surveillance;
* requirements that any recorded surveillance data or images be stored in a secure manner, including guidelines for managing video surveillance recordings, such as security, use, disclosure, and retention and appropriate details on the place where signals from the equipment will be received and monitored;
* designations of the persons in the organization authorized to operate the system, including the names of the individuals who may have viewed the surveillance and what the surveillance was used for; and
* requirements that appropriate training is provided to operators to make certain that they understand their obligations under all relevant legislation including *ATIPPA, 2015*, these Guidelines, and the organization's video surveillance policy.

Interesting Cases from Other Jurisdictions

Order F15-29

Summary An applicant requested records from Langara College relating to complaints made against him as well as complaints he had made. The College withheld some identifying information of complainants and witnesses and some other personal information as relating to law enforcement investigations under s. 22 of FIPPA. The adjudicator determined that s. 22 of FIPPA applied to some of the withheld information in dispute. However, the adjudicator found that it was not unreasonable to disclose information that the applicant already knew. https://www.oipc.bc.ca/rulings/orders/1812

New Roles of the OIPC

The *ATIPPA, 2015* brought with it many changes to the role of the OIPC.

New powers

* Auditing compliance;
* Education;
* Own motion privacy investigations;
* Approval of all time extensions;
* Approval required to disregard access requests;
* Final decision on fees;
* Reviewing PIAs for common or integrated programs or services;
* Filing court orders in relation to reports;
* Engage in and commission research; and,
* Authorizing Indirect collection of Personal Information.

Clarification of previous authority

* Reviewing solicitor client records;
* Reviewing most exempted records;
* Reviewing cabinet confidences;
* Conducting privacy investigations; and,
* Banking of complaints when there are 5 active complaints from the same applicant that deal with similar or related records.

Quick Tips

When using discretionary exceptions, don't forget to check if the public interest override applies.

If a complaint is filed at the OIPC, your first response should include your representations and is the best opportunity to explain why it is your position that the exception applies to the record.

The initial consultation with a Third Party (seeking their consent to release) does not stop the clock on responding to the access request. It is only if the Third Party objects to the release and files a complaint with the OIPC that the clock stops.

All time extensions must be approved by the OIPC.