ABOVE BOARD

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

VOLUME 10, ISSUE 01 JANUARY 2018

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

[There is] an onus on individuals to look out for themselves – to be masters, so to speak, of their own data. But in order to share only the information they want to share – and only with those friends they want to share it with – people need to be able to exercise a meaningful level of control over their personal information."

Jennifer Stoddart, former Privacy Commissioner of Canada

OIPC REMINDERS AND UPDATES

Data Privacy Day 2018

We dedicate this issue of Above Board to privacy-related topics as we celebrate and raise awareness of Data Privacy Day, 2018.

Data Privacy Day is observed annually on January 28 and was first observed in Canada in 2008 in recognition of Data Protection Day celebrations in Europe. The European celebration marks the signing of Convention 108 on January 28, 1981. Convention 108 was the first legally binding international treaty relating to privacy and data protection.

To mark the occasion, the OIPC produced a Data Privacy Day poster. Additionally, the International Association of Privacy Professionals (IAPP) will host a Privacy After Hours event at Bitters Pub at 7p.m. on Wednesday, January 31, with trivia hosted by the OIPC to follow at 8 p.m. The event is open to both IAPP members and non-members. Come join us for a fun night out! Trivia questions will be general knowledge, with some punny categories.

For more information you can visit our website, the official Data Privacy Day website or the federal Privacy Commissioner's website.

Privacy Training from the OIPC

The OIPC is available to deliver training on privacy-related matters and issues. Training can focus on the privacy provisions of the *ATIPPA, 2015* or can be tailored to a particular concern or topic as requested.

To arrange for an education session for your organization contact:
commissioner@oipc.nl.ca

ANONYMITY OF APPLICANTS

Section 12 of the *ATIPPA, 2015* requires that the name and type of applicant remain confidential throughout the ATIPP request process and may only be disclosed to certain individuals within the public body (i.e the coordinator, back-up coordinator(s) and the coordinator's assistant(s)). There are limited exceptions.

Preserving an applicant's anonymity is grounded in the duty to assist. By limiting the number of individuals who are entitled to know the identity of the applicant, requests can be processed in a fair, open, accurate and complete manner. Anonymity must extend not only to the full name of the applicant, but also the type of applicant regardless of whether it may be possible to infer the identity of the applicant.

Anonymity must be afforded throughout the entirety of the request process inclusive of consultations and third party interactions. Furthermore, in accordance with section 68 of the *ATIPPA, 2015* unless the identity of the applicant becomes necessary in relation to one of the permitted disclosures, it should not be disclosed after the request process is finished. It is important for public bodies to understand that even permitted disclosures of an applicant's identity must be limited to the extent necessary to respond to the request.

Additionally, while public bodies are encouraged to designate a back-up coordinator and assistant, this designation should not be taken to mean that the identity of the applicant should routinely be disclosed to those individuals. The identity of the applicant should only be disclosed to those individuals where it is necessary to respond to the request.

Measures to Assist in Ensuring Anonymity

1. Always refer to an applicant as "the applicant" or by an assigned request number.
2. Remove the name and address of the applicant on all correspondence related to the request to be sent between anyone other than the applicant and coordinator.
3. Only after the final response has been approved by the Head of the Public Body should the letter containing the name and address of the applicant be presented for signature by the Head.
4. If an access request is made by an employee, documents associated with the request should not be placed on the employee's personnel file.
5. Ensure that any verbal or written references to other on-going or past requests by the applicant of any type do not reveal the identity of the applicant.
6. Restrict access to ATIPP request documents, both electronic and paper.
7. Ensure any written search instructions do not contain personal information. De-identify the wording of the request, where necessary.
8. Develop and implement a policy regarding preserving the anonymity of applicant.

You can review the full guidance piece on our website

RESPONDING TO A PRIVACY BREACH — KEY STEPS

STEP 1: *Contain the breach*. Do what is necessary to limit the breach and begin your investigation. Notify internal privacy and security personnel, the OIPC and the police if necessary.

STEP 2: *Evaluate the risks.* Identify the information involved and the sensitivity of the information. The more sensitive the information, the higher the risk. Identify the cause and extent of the breach including number of victims and the number of recipients; the identity of the recipients; the risk of further access, use or disclosure; whether the information was lost, stolen or accessed; whether the information was encrypted; whether the information was recovered; and whether the breach was an isolated incident. Identify the type of harm that may occur including, but not limited to, physical safety, identity theft, loss of business, emotional distress or damage, loss of trust, loss of contracts, and financial losses.

STEP 3: *Notification.* Notification should occur as soon as possible following a breach, unless the breach does not create a risk of significant harm to the individual affected. Direct notification is preferable. Notification should include: date of the breach; a description of the breach and the information involved; any identified risks; the steps taken in relation to the investigation and breach containment; any identified future steps; any steps the individual can take; as well as any steps the public body is offering to assist the individual in mitigating the harm. The notification should also contain the contact information for the public body and for the OIPC, along with informing the person of the right to file a privacy complaint.

STEP 4: *Prevention*. Evaluate the physical, technical, administrative and personnel safeguards currently in place and augment them accordingly to prevent future breaches.

Steps 1-3 should be undertaken immediately upon discovery of the breach. Step 4 should occur after the cause of the breach is identified to prevent future breaches.

PROTECTING YOUR ONLINE PRIVACY

Social media is a valuable and useful tool for sharing information, knowledge and opinions. Most of us use social media on a daily basis to communicate with friends and loved ones. In any use of social media, it is important to properly manage and protect your personal information. Below are some quick tips on how to protect your online privacy.

- Limit the amount of personal information you provide when setting up your account. Likewise, limit the amount of personal information you share online.
- Be conscious of who can see your personal information (e.g. scrutinize “friend” requests to be certain the account holder is actually an individual you know and trust).
- Limit the number of platforms used and delete any inactive accounts.
- Familiarize yourself with, use, and if necessary, adjust the privacy settings of the platform.
- Use strong password protection.
- Ensure photos do not contain geotags.
- Be cautious when posting information that when coupled with other available information can be used for a malicious purpose (e.g. posting that you need a dog-sitter for a specified time period, posting a check-in at the airport and posting vacation photos).
- You should also be aware of your use of other people’s personal information.

WHO IS RESPONSIBLE FOR PRIVACY?

Privacy, and the larger subject of information protection, is everyone's responsibility. So what can you do to change perceptions and promote collaboration?

Get Support from the Top

Under the *ATIPPA, 2015*, it is the head of the public body that is accountable for ensuring personal information is protected, among other requirements. While the head may designate an individual to be responsible for the day-to-day management of this task, they retain accountability. The head should ensure that the public body's executive is aware of privacy obligations and that the entire management team publicly demonstrates support for privacy initiatives.

Resource Adequately

Individuals with delegated responsibilities for privacy require a variety of resources. First and foremost, they need training in privacy, including legislation and available tools. They also need to be able to dedicate adequate time to privacy. While some time will be spent on privacy complaints and breach reports, time should also be devoted to proactive initiatives, such as developing a privacy management program and writing privacy impact assessments (PIAs).

Build an Inner Circle

Everyone has a role to play. Managers and directors, especially those overseeing programs and staff that collect, use and disclose personal information, are responsible for ensuring appropriate policies and procedures are in place and their staff are aware of privacy expectations. Individuals responsible for privacy should also have close ties with the ATIPP Coordinator, and professionals involved in information management, information technology, security, risk management, human resources and policy.

Develop a Privacy Education Program

Public bodies should offer training and awareness activities to educate all staff and contractors on privacy obligations and affiliated policies and procedures. These programs should also promote the role everyone plays in protecting personal information such that all staff are aware of their responsibilities. Use training and awareness activities to ensure everyone understands their own role in protecting personal information. Remind them that the information they are protecting, in many cases, includes their own personal information and/or that of family, neighbours and friends.

Collaborate

Privacy requires collaboration. It takes an entire organization, from the bottom to the top, to ensure that personal information is protected. If anyone in your organization can cause a breach, then everyone has a role to play in protecting personal information. When everyone works together to protect personal information, everyone benefits.

COLLECTING INFORMATION VIA SOCIAL MEDIA (EMPLOYEE AND BACKGROUND CHECKS)

Public bodies may want to obtain personal information from social media in a number of contexts, including:

- vetting employment candidates; or
- monitoring the conduct of current employees.

A social media employee or background check can include a variety of activities ranging from checking a Facebook profile to searching all platforms for all information about an individual. Collecting personal information via social media is a form of indirect collection and section 62 (1) of the *ATIPPA, 2015* requires public bodies to collect personal information directly from individuals unless indirect collection is permitted by the *Act.*

Vetting Employment Candidates

Public bodies should avoid collecting and using information obtained from social media due to a growing set of concerns with the content of social media.

Information on social media can be inaccurate, unreliable, untruthful and out-of-date. Accounts are easily obtained and replicated, sometimes by imposters. The *Act* requires that public bodies take all reasonable measures to ensure the accuracy of personal information if it is to be used to make a decision about a person.

Additionally, it is likely that public bodies will encounter irrelevant and possibly prejudicial information about an employment candidate and, possibly unintentionally, allow that information to cloud their judgment and assessment of the individual. Depending on the nature of the information, a public body may also have to defend against allegations of discrimination.

Furthermore, it has been recognized that reasonable expectations of privacy can exist despite individuals sharing personal information in circumstances where they have limited control over who has access to it. (R. v. Marakah, 2017 SCC 59 (CanLII)).

Monitoring the Conduct of Current Employees

Public bodies can require that employees adhere to reasonable policies regarding the acceptable use of social media. Employees authorize the indirect collection of their personal information by accepting employment according to its terms and conditions, including social media policies, if notified at the time of hire. Public bodies must ensure that employees are aware of their social media policies and the potential consequences for violating those policies.

Public bodies can indirectly collect information via social media to identify potential instances of non-compliance. Arguably, the collection relates directly to and is necessary for activities of public bodies in accordance with the *Act.*

(Continued on next page)

COLLECTING INFORMATION VIA SOCIAL MEDIA (EMPLOYEE AND BACKGROUND CHECKS) (CONTINUED)

Public bodies checking employee's social media activities must bear in mind all of the above-noted issues regarding reliability, accuracy, relevancy, discrimination and impacts on third parties.

Individuals who believe on reasonable grounds that their personal information has been collected, used or disclosed by a public body contrary to the *Act* can complain to the Commissioner pursuant to section 73. The Commissioner can also commence an own motion investigation into such matters. Also, individuals have a right to request access to the information collected and used by a public body to make a decision about a candidate or employee.

This guidance does not apply to information collected via social media for the purposes of law enforcement, defined in section 2(n) of the *Act*.

You can review the full guidance piece on our website

PRIVACY MANAGEMENT PROGRAM FRAMEWORK

The OIPC has created a Privacy Management Program framework designed to provide step-by-step guidance on how public bodies can implement effective and accountable privacy management programs. A privacy management program ensures that privacy is built into all initiatives, programs or services. The framework will soon be accessible on our website.

If you have any questions or would like further direction please contact the Office.

PRACTICE TIP

If your organization does not have a security protocol requiring regular and frequent password changes, ensure that employees are changing their passwords on a set timeframe. Include guidance on creating strong and secure passwords, including the use of upper and lower case letters, special symbols and numbers.

THE MORE YOU KNOW...

Below are links to the privacy policies and information on some of the more frequently used social media sites:

Facebook Data Policy
Facebook Privacy Basics
Linkedin Privacy Policy
Snapchat Privacy Policy
Snapchat Safety Center
Twitter Privacy Policy

http://socialmediagovernance.com/policies/ lists the social media policies of more than 240 organizations worldwide.

ATIPPA PRIVACY BREACH STATISTICS Oct. 1 - Dec. 31, 2017

During this reporting period (October 1— December 31, 2017), the OIPC received 59 privacy breach reports from 20 public bodies under the *ATIPPA, 2015*. This is up from the 40 reports from 15 public bodies received in the previous reporting period.

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 St. John's	2
College of the North Atlantic	3
Dept. of Advanced Education, Skills & Labour	7
Dept. of Children, Seniors & Social Development	4
Dept. of Education & Early Childhood Development	1
Dept. of Finance	1
Dept. of Fisheries & Land Resources	1
Human Resource Secretariat	5
Dept. of Justice & Public Safety	2
Dept. of Service NL	10
Dept. of Transportation and Works	1
Eastern Health	4
Executive Council	1
Newfoundland and Labrador English School District	3
Newfoundland and Labrador Housing Corporation	3
Newfoundland and Labrador Legal Aid Commission	4
Public Service Commission	1
Town of Labrador City	1
Town of Lewisport	1
Workplace NL	4

Summary by Type	
Email	22
Other	12
Mail Out	12
In Person	8
Intentional (i.e. willful breach)	3
Technical Malfunction	2

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