ABOVE BOARD

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

Volume 15, Issue 1 January 2023

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:

Data Privacy Day – January 28, 2023

January 28, 2023, is Data Privacy Day. It is an internationally recognized day, dedicated to creating awareness about the importance of privacy and the protection of personal information.

The first Data Privacy Day was recognized in Canada in January 2008 as an extension of the Data Protection Day celebration in Europe. Data Protection Day commemorates the January 28, 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection.

Data privacy can be defined in many different ways, but one basic element is the right to control who gets to see your personal information. With technology changing at an increasingly fast pace, controlling who can collect, use and disclose your personal information is becoming more difficult. More and more personal information is being collected and used, potentially affecting your right to privacy. Individuals need to be more conscious of what information they are providing and take steps to protect personal information.

Privacy has been recognized by the Supreme Court of Canada as a right of all Canadians under the Charter of Rights and Freedoms. In this Province privacy is protected by law through the *Access to Information and Protection of Privacy Act, 2015* and the *Personal Health Information Act*.

For Data Privacy Day, the OIPC has developed a video with Commissioner Michael Harvey explaining your privacy rights under Newfoundland and Labrador law. To view this video, please visit www.oipc.nl.ca/events/data-privacy-day.

Data Privacy Day encourages everyone to own their privacy responsibilities to create a culture of privacy!

Privacy Breach Resource for Individuals

The *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*) regulates how public bodies can collect, use and disclose your personal information. Public bodies must have a purpose to collect, use or disclose your personal information but in doing so they must limit it to the minimum amount necessary.

A privacy breach happens when your personal information is not handled properly by a public body. A public body employee might look at your personal information for no legitimate purpose or an email including your personal information could be sent to the wrong individual. These are examples of privacy breaches.

If you have been notified by a public body that your privacy has been breached, your first question is likely to be what information was involved. In trying to get more detail about the information that was affected, it would be best to contact the public body that sent you the notification. Public bodies have employees designated to deal with privacy breaches. If you believe your privacy has been breached but have not been notified then you can contact the public body you believe has breached you privacy.

A few examples of things you can do to help protect yourself if your privacy has been breached are:

- limit the amount of personal information you share;
- asks questions of the organization collecting your personal information including reasons why they need it;
- use strong passwords;
- if your financial information has been breached contact your bank or credit monitoring service to let them know.

The ATIPP Office at the Department of Justice and Public Safety has created a useful resource which can be found here "Protection of Privacy - What to Do if your Personal Information is Breached".

Is Someone Watching? Tips for Securing Web-connected Cameras

Web-connected cameras have become increasingly popular and while many people find them convenient, they do come with privacy risks. The Office of the Privacy Commissioner of Canada (OPC) noted that it is surprisingly easy for people to tap into web-connected cameras and while some cameras show outdoor spaces, others cameras are located inside your home or other private areas. The OPC said that internet-connected devices with a camera such as baby monitors, laptop cameras, and home security systems can be easily hijacked to allow random strangers to watch intimate moments. These internet-connected devices can also give away details about your location and movements.

The OPC noted that taking a simple step like changing the default password can help reduce the likelihood of someone using your camera to spy on you. Below are tips from the OPC to help prevent your web camera from being live-streamed:

Research - The OPC advised that before purchasing a smart device or downloading an app you should learn about what personal information is being collected and what privacy controls are available. The OPC said to "Be wary of companies offering products and services with no privacy protection information, or incomplete information. This should raise a red flag." Individuals can also

enter the camera make and model into a search engine to see if there are any security related posts available. The OPC also said to ensure there is a way to update the firmware on the camera by reviewing the operating instructions.

Change Passwords - The OPC advised that one of the principal ways other people can access your internet-connected cameras is through the manufacturer's default password, which can easily be found online. The OPC recommended the following steps:

- change the default password;
- use a secure password, with two-step authentication if possible;
- do not use the same passwords across devices;
- verify that the password is changed instead of a new account being created with the old password still active. After changing the admin password, attempt to login using the old password. You should not be able to do so.

Secure Router - The OPC advised changing the password on your router as hackers can use weak router passwords to gain access to all your devices.

Disable Camera and Microphone - When your camera in your device is not in use, you can use a sticky note or camera cover to cover the camera lens. Ensure your device is set up to let you know when information is being collected, such as a light to let you know the camera is on. Additionally, if the camera and microphone in your device is not needed at all then you can disable them.

Additional tips from the OPC:

- do not take your web-connected camera into especially sensitive areas such as bedrooms or bathrooms;
- be camera-aware – know whether it is on and where it is pointing;
- be mindful about the access that children may have to the camera to ensure they do not inadvertently turn the camera and microphone on by themselves;
- make sure outdoor security cameras do not give away information like street number or licence plate;
- only activate the functions you need or want, and favour devices that clearly indicate when information is being collected;
- do not click on suspicious links, which can download viruses and let hackers into your system.

Protecting Privacy on Social Media

Social media is everywhere and it can tell others a lot about you if they know where to look. The more you share on social media, the more information about your life can be stolen.

Don't Share your Live Location or Daily Routines

Posting details about live locations and daily routines may seem innocent, however, they could be used to track your movements and could alert thieves as to your whereabouts. For example, advertising that you're on vacation alerts everyone that you are away from home. Instead, post your vacations pictures once you are home. Similarly, posting where you get your coffee every morning and at what time can tell people where to find you and when you will be away from your house.

Never Share Identification Numbers

Sharing identification numbers can have drastic consequences! Sharing your social insurance number, driver's licence, bank account numbers and passports hands thieves the tools to steal your identity.

Personal Information & Contacts

When posting information about yourself online, you don't need to share everything. The more you share, the bigger your online footprint. Not every field has to be filled in and not every field requires detailed personal information. Look at what is required and consider using more broad information. Also, only accept requests from people you know. The more personal information you share, the more information is available to hackers to help them hack your security questions for your accounts.

Delete Expired Social Media Accounts

No longer using it? Then there is no need to keep it. Every account you keep adds to your vulnerability.

A Long Password is a Strong Password

Passwords are almost the first thing you enter into your social media accounts. Making them as secure as possible will help protect your information. Don't use common passwords or specifics about yourself or family members like birthdays or pet names. Generally, a long password is a strong password. A password with 12-16 characters including extra characters is a good place to starts. Also, a different password for each account helps limit hackers if one account is compromised.

Two-Factor Authentication – Always a Good Idea

Two-factor authentication is a security measure that requires a one-time code that is usually only valid for a short period of time. Since the code and the right device are required this makes them more secure.

Security Alert Emails

Pay attention to any emails about the security of your devices. Notifications of failed logins or attempts at changing passwords can be warnings signs of a hacking attempt. Also, read the email fully to ensure if it not a scam or phishing attempt.

Protection in Public Places

Using public wifi for transactions is risky as hackers can intercept your connection and collect the data. Also, be aware of who is close by as they could be shoulder surfing, people who lurk close while you are entering your password for a social media account. It is not just online security you need to watch for but also physical distancing when entering passwords in public.

Recent Joint Resolutions from Privacy Commissioners

Two new joint resolutions from Privacy Commissioners and Ombudspersons with responsibility for privacy oversight were approved and issued in the Fall of 2022, both relating to digital aspects of privacy. One was in relation to Trust in Digital Healthcare and the other was in relation to Privacy and Transparency in the Digital Identity Ecosystem.

Regarding healthcare, Commissioners made a series of recommendations to governments and health care providers to modernize their health information systems and legislative frameworks so that they meet the privacy principles that are enshrined in health information statutes across the country as well as meeting the high standard of protection against breaches.

Regarding digital identity, Commissioners made a series of recommendations to governments and relevant stakeholders to ensure that rights to privacy and transparency are fully respected throughout the design, operation and ongoing evolution of a digital identity ecosystem in Canada. The joint resolution included a non-exhaustive list of conditions and properties, including ecosystem properties, individual rights and remedies, and governance and oversight, that should be integrated with a legislative framework applicable to the creation and management of digital identities.

To read the full joint resolutions please visit:

Securing Public Trust in Digital Healthcare - Office of the Privacy Commissioner of Canada;

Ensuring the Right to Privacy and Transparency in the Digital Identity Ecosystem in Canada - Office of the Privacy Commissioner of Canada.

Artificial Intelligence and Privacy

There are varying definitions for artificial intelligence (AI)[1] but it is generally understood to be a kind of machine learning that can perform tasks that normally require human intelligence.
One of the clashes between AI and privacy has to do with personal information. AI needs sufficient data for its training and learning processes and depending on what it is learning, personal information could easily be involved. The protection of personal information usually depends on limitations and disclosing only what is necessary. How can AI and privacy co-exist? The answer is not yet clear.

To delve into a discussion on AI please listen to the podcast on Cross Talk CBC Radio 1 about Artificial Intelligence that aired on January 4, 2023. Commentary from Sean Murray, Director of Research and Quality Assurance at the OIPC and Stephen Czarnuch, Director of the MUN Centre for Artificial Intelligence will help explain different aspects of AI and privacy and promote further thought on the matter.

Please listen to the podcast here:

https://www.cbc.ca/listen/live-radio/1-89-crosstalk/clip/15957819-artificial-intelligence-rare-bird-sighting-labrador.

[1] "Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector" (Joint Special Report No. 2, June 2021) online: https://www.oipc.bc.ca/special-reports/3546.

ATIPPA, 2015 Privacy Breach Statistics October 1 – December 31, 2022

During the last quarter of 2022 (October 1 to December 31, 2022), the OIPC received 49 privacy breach reports from 23 public bodies under *ATIPPA, 2015*. This is an increase from the 33 breaches reported during the previous quarter.

More than half the breaches remain as email breaches. The last issue of this newsletter (October 2022) included tips to help employees reduce or prevent email-related breaches. Please review these tips here www.oipc.nl.ca/pdfs/AboveBoardOctober2022.pdf.

There was one intentional breach reported by the Royal Newfoundland Constabulary (RNC) whereby an employee accessed a file relating to a workplace motor vehicle accident that they were involved in. The matter was to be reviewed by the employee's manager and the RNC would be conducting an internal investigation.