ABOVE BOARD

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

Volume 16, Issue 1 January 2024

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

Website:
www.oipc.nl.ca

Follow us on social media!

Twitter:
@oipcnl

New!
LinkedIn:
https://Linkedin.com/company/oipc-nl

This Issue:

Data Privacy Week 2024

Data Privacy Day is **January 28, 2024**!

Data Privacy Week is **January 22-28, 2024**!

Data Privacy Day (DPD) is an internationally recognized day, dedicated to creating awareness about the importance of privacy and the protection of personal information. DPD commemorates the January 28, 1981 signing of Convention 108, the first legally binding international treaty dealing with privacy and data protection. DPD celebrations now expand to a full week taking place this year from January 22-28, 2024.

We live in an increasingly digital world and technological advances continue to impact privacy and the protection of our personal information. Data Privacy Week provides our Office with the opportunity to emphasize that safeguarding your personal information should be a priority!

Most people do not think about data privacy until it is too late and their personal information has been compromised. Data Privacy Day is an important reminder to those who may think that having spam software and a firewall is enough to protect their data in today's digital world. Individuals need to rethink what information they share, when they share it and to whom.

While the OIPC doesn't like to think about personal information as a commodity, increasingly the world economy is treating it that way. Your personal information has value – you need to protect it and have a right to

have it protected by public bodies, custodians and businesses that hold it in trust for you.

OIPC Data Privacy Week Events

We are kicking off Data Privacy Week by extending a friendly challenge to our province's Access to Information and Protection of Privacy (ATIPP) Coordinators and Custodians by putting their knowledge of privacy related topics to the test in the form of our Crossword Puzzle and Multiple Choice Quiz.

Information and Privacy Commissioner Michael Harvey will also be discussing Data Privacy Week and privacy topics, including privacy rights of youth and employee privacy, on VOCM's News Talk (Monday, January 22, 2024 at 4PM and CBC's The Signal (Thursday, January 25, 2024 at 12PM)

Privacy and Artificial Intelligence

In December 2023, the Privacy Commissioner of Canada announced a new set of principles to address the use of Artificial Intelligence (AI) taking into account privacy implications at the international Privacy and Generative AI Symposium. Federal, provincial and territorial privacy authorities, including Newfoundland and Labrador's OIPC, released these principles to advance the responsible, trustworthy and privacy-protective development and use of generative AI technologies in Canada.

The regulators noted that while AI presents potential benefits, there are also risks and potential harm to privacy, data protection, and other fundamental rights if the technologies are not properly developed and regulated. Organizations have a responsibility to ensure that products and services that are using AI comply with existing domestic and international privacy legislation and regulations.

The documents outline how key privacy principles apply when developing, providing, or using generative AI models, tools, products and services and include:

- Establishing legal authority for collecting and using personal information, and when relying on consent, ensuring that it is valid and meaningful;
- Being open and transparent about the way information is used and the privacy risks involved;
- Making AI tools explainable to users;
- Developing safeguards for privacy rights; and
- Limiting the sharing of personal, sensitive or confidential information.

The document provides examples of best practices, including implementing "privacy by design" into the development of the tools, and labelling content created by generative AI.

The entire document is available here Principles for Responsible, Trustworthy and Privacy-Protective Generative AI Technologies.

An Overview of Employee Privacy

In the October 2023 edition of *Above Board*, we detailed the annual meeting of the federal, provincial and territorial (FPT) Information and Privacy Commissioners and Ombudspersons which took place in Québec City from October 3-6. Among the three joint resolutions signed during the summit was *Protecting Employee Privacy in the Modern Workplace*, a resolution which addressed the recent proliferation of employee monitoring software and the shortcomings of current privacy laws tasked at safeguarding workers from overly intrusive employer surveillance.

The Rise of Workplace Surveillance

Employee surveillance is not a new concept. Monitoring workers to evaluate performance, assess compliance with organizational polices and meet legal responsibilities has been an underpinning of capitalist work for hundreds of years. Propelled by technological expansion, however, workplace surveillance methods have become increasingly efficient and intrusive over time, and by the late 1990's, visual monitoring, time stamps and time clocks had given way to the electronic monitoring of email messages, computer file access and internet browsing. The 2015 review of Newfoundland and Labrador's *Access to Information and Protection of Privacy Act* (*ATIPPA*) noted that surveillance technology was now part of working life and that personal information was often poorly protected in the workplace, opening the door for serious privacy violations.

In times of societal crisis, studies show that surveillance use dramatically increases in both pace and intensity, a fact supported by the speed and thoroughness with which employers adopted innovative monitoring and surveillance technology in response to the Covid-19 pandemic in 2020. This, in turn, prompted an enhanced capability to collect precise, minute details about an employee's actions, progressively encroaching upon individual privacy rights by intruding increasingly further into an employee's private space. Traditional employee surveillance techniques were supplanted by electronic behavior tracking and electronic performance measuring tools, including facial recognition software and Artificial Intelligence (AI), which frequently lacked user transparency and safeguards to alert them when such tools were being used, what personal information was being collected and for what purposes. These technologies, which gather and quantify especially sensitive and confidential biometric information, such as eye movement, mood and tone of voice, facilitate invasive surveillance. Such surveillance extends beyond legitimate workplace monitoring purposes such as ensuring productivity, safety, compliance with regulations and company policies.

In addition to the unprecedented impact on personal privacy, excessive employee surveillance using innovative digital monitoring technology has been shown to negatively impact individual self-esteem and lead to anxiety, depression, loss of dignity and a diminished sense of autonomy. Such stressors on workers foster a relationship with employers which can cause disengagement, low morale, high turnover and the prevalence of an overall culture of distrust. Further, there are indications that marginalized and vulnerable communities are particularly susceptible to digital workplace monitoring and disproportionately impacted by its intrusive effects.

The Current Employee Privacy Landscape

Legislative protections for employee privacy are uneven across jurisdictions and employment sectors.

Public sector employees are generally provided privacy protections and oversights under provincial and territorial public sector privacy legislation, such as Newfoundland and Labrador's *ATIPPA, 2015*. At the federal level, similar protections are offered under the federal *Privacy Act* and, for federally regulated industries (e.g. airlines and interprovincial transportation services, postal and courier services, radio and television broadcasting) protections are provided under the federal *Personal Information Protection and Electronic Documents Act* (*PIPEDA*). Under these statutes, employee information, even under these statutes, is treated differently than personal information but not explicitly defined. For example, an employee's business contact information, unlike their personal contact information, is not considered personal information. Their name would not be considered personal information if it is used in the context of the conduct of their public sector employment. Nevertheless, other aspects of their personal information have some protection and independent oversight is available through privacy commissioners.

Comparable protections are available to private sector employees in only the three provinces which have private sector privacy legislation: British Columbia, Alberta and Quebec. These statutes define employee personal information specifically and distinguish it from personal information collected outside an employment context. Each of these statutes provides for oversight by the Commissioners in each jurisdiction.

The largest gap for employee privacy is the absence of protections for private sector workers not employed in federally regulated industries in the seven provinces and three territories – including NL - without stand-alone private sector privacy laws. The lack of protections for this sub-group is particularly concerning considering it undoubtedly includes a significant proportion of service industry jobs, which traditionally are overrepresented by workers from marginalized populations.

There are several other legal protections against intrusive surveillance practices available to Canadian workers. The *Canadian Charter of Rights and Freedoms*, the *Criminal Code of Canada*, the *Canada Labour Code*, human rights legislation, union negotiated collective agreements and employment contracts are all potential options. Yet, the circumstances under which each option is applicable and available are often difficult to ascertain, and their effectiveness in providing protections can be varied and situational. For example, the *Charter's* protections are confined to only government actions, which unto itself can be a difficult concept to define. Additionally, the *Criminal Code of Canada* allows for the interception of communications through surveillance in an employment context if express or implied consent is provided. Given the aforementioned unequal power distribution in the employer-employee relationship, particularly among marginalized workers, the legitimacy and meaningfulness of any consent ultimately given for surveillance in such an instance would be in question.

Ultimately, these legislative gaps and shortcomings serve to exacerbate surveillance-related impacts on employee privacy, well-being and job satisfaction, but they also prove inadequate to Canada's Information and Privacy Commissioners, Ombudspersons and its courts as they attempt

to provide oversight, resolve disputes and balance individual privacy rights against legitimate employer business interests.

A Human Rights Approach to Employee Privacy and Legislative Reform

In his October 6, 2023 press release announcing the FPT joint resolution, Commissioner Harvey remarked that invasive employee surveillance is in direct opposition to a human rights approach to privacy. Given the potentially harmful consequences surveillance poses to worker autonomy, dignity and overall health and well-being, it is essential that any measures, legislative or otherwise, aimed at protecting workers from such intrusions on their private space be developed and implemented through a human rights lens. Such an approach was proposed by the joint resolution, through its recommendations to Canadian FPT governments and employers, as the most suitable to address legislative shortcomings and safeguard workers from the impacts of modern workplace surveillance. Accomplishing this goal requires treating privacy, specifically employee privacy, as a priority and affording it the same protections given to other human rights, such as free speech and freedom of expression, from which the right to privacy is inseparable.

A human rights based-approach to employee privacy would involve strengthening legislative protections and incentivizing a privacy-by-design culture by introducing a requirement for responsible deployment of surveillance technologies. This would include ensuring monitoring is reasonable, is legitimately necessary, limits the collection, use, retention and disclosure of personal information to that required to fulfill its demonstrated purpose and restricts any impact on employee privacy to that which is proportional to the demonstrated need. This rights-centric method to privacy reform would also require employer transparency and accountability by way of thorough written and easily accessible surveillance-related policies and procedures, meaningful employee involvement and participation in the development of surveillance practices, and the presence of methods to assess risks and adherence to privacy laws, such as privacy impact assessments and auditing processes. Also necessary would be a robust and equitable conflict resolution process by which employees can dispute the use of surveillance and/or decisions made on the basis of surveillance and seek reparations for biased treatment. Finally, it would be crucial that any new protections or changes to existing protections, whether from a legislative perspective or in the form of recommendations to employers, be consistent across jurisdictions to ensure that all workers are protected equally. These are the same privacy principles embedded in privacy statutes in Canada and much of the rest of the world, with roots in principles agreed upon by the Organization for Economic Cooperation and Development (OECD) more than 40 years ago.

The OIPC will be undertaking additional research and advocacy work on employee privacy in the coming months. Stay tuned to our website and social media for more on this topic.

Privacy Tips for Individuals

Quick Tips to Help Protect Your Privacy

1. Don’t Give Too Much Information

No online store needs your Social Insurance Number (SIN) or your birthday. Safeguard your SIN as it can open the door to your personal information and put you at risk for identity theft. Provide the least amount of information.

2. **Strong and Long Passwords**
   Combine capital and lowercase letters with numbers and symbols for a more secure password. Ensure your passwords are hard to guess.

3. **Banks – Be Aware**
   Financial institutions do not request personal information from customers by unsolicited email, text or telephone calls.

4. **Automate Software Updates**
   Turn on automatic updates if possible as many software programs will automatically connect and update.

5. **Check Security Settings**
   Look at the privacy, security and advanced preferences on your browser to see what information it is storing automatically.

6. **Protect your Money**
   When banking and shopping, check sites to ensure security is enabled.

7. **Checking In**
   Frequent check-ins online can put your privacy at risk.

8. **When in Doubt, Don't Respond**
   If an email requires you to act immediately, offers something too good to be true, or asks for your personal information, be wary.

9. **Monitor your Accounts**
   Regularly monitor your account activity. Notify companies involved immediately if you notice suspicious activity.

10. **Wi-Fi hotspots**
    Wireless networks and hotspots are not secure. Limit what you do on public Wi-Fi and avoid logging into your email or bank.

Managing a Privacy Breach (for Public Bodies)

The Access to Information and Protection of Privacy (ATIPP) Office has a Privacy Breach Protocol for public bodies. Please review this guidance for a more detailed explanation when handling privacy breaches.

Here are quick reminders of the steps to take and questions to ask when responding to a privacy breach:

Step 1 - Contain the Breach

- Immediately stop the unauthorized practice;
- Recover the records; and
- Correct weaknesses in physical security.

Additional Steps:

- Immediately contact your supervisor;
- Submit Privacy Breach Reporting Form to your Senior Privacy Analyst with the ATIPP Office and the OIPC; and
- If there is a risk of criminal harm, contact the RNC or RCMP.

Step 2 - Evaluate the Risks

Information Involved:

- Was personal information involved in the breach?
- What types of information were involved in the breach? (The more sensitive the information, the higher the risk.)
- Can the information be used for fraudulent or otherwise harmful purposes? (Social Insurance Numbers and financial information, for example, can be used for identity theft).

Cause and Extent of the Breach:

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- How much information was collected, used or disclosed without authorization?
- How many individuals are likely to receive or have access to the information that was breached?
- Is the information protected by encryption or other means rendering it not readily accessible?
- What steps have already been taken to minimize the harm?

Who was Affected by the Breach:

- How many individuals are directly affected by the breach?
- Who was affected by the breach: employees, citizens, clients, other public bodies?

Foreseeable Harm from the Breach:

- Is there any relationship between the unauthorized recipients and the information involved in the breach?
- What is the risk of harm to affected individuals as a result of the breach?
- What is the risk of harm to the public body as a result of the breach?
- What is the risk of harm to the public at large because of the breach?

Step 3 - Notification

- If there is a risk of significant harm cause by the breach, you are required to notify the individual(s) affected;

- Notify the ATIPP Office and the OIPC when a privacy breach occurs and submit a privacy breach reporting form;
- If notification is to take place, it should occur as soon as possible following the breach; and
- The preferred method of notification is direct (i.e. by phone, letter or in person) to affected individuals.

Step 4 - Prevent Future Breaches

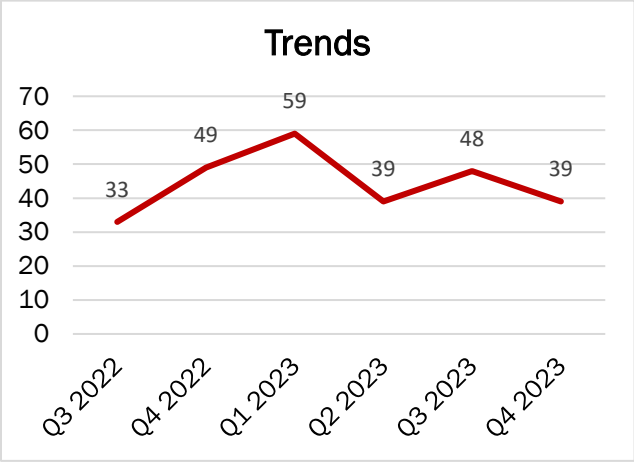
- Thoroughly investigate the cause of the breach -- this could require a security audit of both physical and technical security;
- Develop or improve, as necessary, adequate long-term safeguards against further breaches;
- Review your policies and update them to reflect the lessons learned from the investigation;
- Audit at the end of the process to ensure that the prevention plan has been fully implemented; and
- Ensure all staff are trained to know the organization's privacy obligations under *ATIPPA, 2015*.

For more information on privacy protection and privacy breach protocols, please visit the ATIPP Office website.

ATIPPA, 2015 Privacy Breach Statistics October 1 – December 31, 2023

During the third quarter of 2023 (October 1 – December 31, 2023), OIPC received 39 privacy breach reports from 19 public bodies under *ATIPPA, 2015*. This is a decrease from the 48 breaches reported during the previous quarter. Similar to previous quarters, email breaches continued to be the most common types of breaches, accounting for over half the breaches. When sending emails, remember to confirm the full email address before you hit send, delete pre-populated addresses and use the bcc field for mass electronic mail outs.

Summary by Public Body	
Central Health	2
City of St. John's	3
College of the North Atlantic	2
Department of Children, Seniors and Social Development	1
Department of Digital Government and Service NL	3
Department of Education	2



Department of Environment and Climate Change	1
Department of Health and Community Services	2
Department of Justice and Public Safety	2
Executive Council	1
House of Assembly	1
Memorial University	3
Newfoundland and Labrador English School District	5
Newfoundland and Labrador Housing Corporation	2
NL Hydro	2
Public Service Commission	1
Royal Newfoundland Constabulary	4
Treasury Board Secretariat	1
Western Health	1