Technology's Impact Upon Employee Privacy

This document provides guidance to government institutions and local authorities on how they collect, use and disclose employee personal information.

UPDATED MAY 2024

Office of the
Saskatchewan Information
and Privacy Commissioner

Technology's Impact Upon Employee Privacy

DISCLAIMER: This document is not intended to provide legal advice and is provided for informational use only.

Updated May 2024

Introduction

The Freedom of Information and Protection of Privacy Act (FOIP) and *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) provide employees of government institutions and local authorities with a right to informational privacy in the workplace.

Technology has enhanced how workplaces can organize themselves and how to complete tasks. However, technology can have a significant impact upon employee privacy.

This document provides guidance to government institutions and local authorities on how they collect, use and disclose employee personal information.

Notification of Purpose and Function Creep

Government institutions and local authorities must inform individuals of the purpose for which their personal information is being collected when they are collecting personal information directly from the individual (subsection 26(2) of FOIP and subsection 25(2) of LA FOIP). Therefore, prior to using technology in the employment lifecycle, including monitoring employee activities, government institutions and local authorities must know the purpose for which they are collecting employee personal information. Then, prior to or at the time of collection, the government institution or local authority must inform employees of the purpose.

However, the use of technology in the employment life cycle often occurs as a result of "function creep." Function creep occurs when information is used for a purpose that is not the originally specified purpose. For example, a workplace may install a security system that requires employees to sign-in or sign-out of the workplace. The purpose of the security system is to prevent unauthorized access to a particular workspace. However, organizations may end up using this information to track employee attendance. If organizations do this, they are guilty of function creep. Function creep often is a privacy breach where organizations use and/or disclose personal information without proper authority.

As organizations plan and implement projects, programs or processes, they should be cognizant of the privacy impacts these may have upon employee privacy. Below are some examples of technologies that may impact employee privacy.

Examples of Employee Monitoring Activities

Location-Based Tracking

The location of employees can be tracked through technologies such as Global Positioning System (GPS) devices, radio-frequency identification (RFID) chips and device identifiers such as the media access control (MAC) address and Internet Protocol (IP) address.

GPS

GPS is a satellite-based radio navigation system[1]. Many devices have GPS capabilities that can reveal the longitude, latitude and altitude of the device. Organizations can track the location of their employees through GPS devices, including by installing GPS devices into vehicles or tracking mobile devices.

RFID Chips

An RFID chip reader broadcasts a radio, which prompts a nearby RFID chip to transmit data to the chip reader.[2] RFID chips with a unique serial number are often installed into employee badges. The RFID chips become activated when an RFID chip reader is nearby. Organizations can use RFID chips and RFID readers to track employee attendance and location.

Device Identifiers

Devices that connect to networks have identifiers such as the MAC address and an IP address. In a workplace where wireless access points are setup, organizations can track employees' mobile devices as employees move around in the workplace.

Tracking Employee Activity

Organizations manage and secure their IT systems by using software to monitor activities that are occurring on their network. However, organizations may use such software for secondary purposes such as monitoring employee activity (personal Internet usage, recording keystrokes, etc.) to determine employee engagement and productivity.

Another method of tracking employee activity is through a system's auditing capabilities. Auditing features may record how employees have interacted with information stored within a system. Typical uses of auditing features include ensuring employees are only accessing information on a need-to-know basis. Before proceeding to use auditing features to track employee activities, organizations should conduct a privacy impact assessment, which is discussed further below.

---

[1] *The Global Positioning System*. Official U.S. government information about the Global Positioning System (GPS) and related topics. https://www.gps.gov/systems/gps/.

[2] *Radio Frequency Identification (RFID) Technology*. Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/02_05_d_28/.

Surveillance

Audio and Video Surveillance

Often, organizations justify installing cameras and/or microphones to conduct audio and video surveillance as a means to protect themselves against unwanted activity (such as theft) and to ensure safety of employees and clients. However, such surveillance means employee activities and conversations are constantly being recorded.

In Investigation Report 034-2015, an individual was concerned about the City of Saskatoon's use of audio surveillance on some of the City's busses. The Information and Privacy Commissioner (IPC) determined that while the City had authority to collect personal information through audio surveillance, he made recommendations on how the City could do so in the most privacy protective manner. He recommended that the City conduct a privacy impact assessment, revise its surveillance policy, revise and increase its signage to notify the public of its use of audio surveillance, and to conduct public consultations about the City's use of surveillance on its busses.

In Investigation Report 090-2017, a bus driver with the City of Saskatoon alleged his privacy was breached when the City used video surveillance footage from a camera installed on a City bus to investigate a complaint that the bus driver hit a cyclist. The bus driver also alleged his privacy was breached when the City used and disclosed footage for the purpose of a grievance hearing. The IPC determined that the City had authority under LA FOIP to use the footage to investigate the complaint and for the purpose of the grievance hearing. He also found that the manner in which the City collected and used the employee's personal information was in compliance with LA FOIP. For example, the City limited its collection and use of the footage to the specific shift in which the employee was driving the bus. It did not access any footage beyond that particular shift.

Data Surveillance

Data analytics is a tool that organizations can use to track employee activities, including with whom they are corresponding and the frequency of the correspondence. Organizations can use such data to gain insights on how work flows through the workplace. The data can also be used for other purposes such as employee performance.

Artificial Intelligence

One form of artificial intelligence (AI) is the use of algorithms to analyze historical data to make predictions about future events. For example, workplaces may use predictive AI to predict which job candidate will likely be the most successful. Workplaces are adopting such AI technologies to assist in the employment lifecycle, including recruiting, hiring and managing employees. However, it cannot be assumed that AI is trustworthy. There are examples of AI being biased, which leads to discriminatory decisions and practices. Furthermore, there are examples of AI being used in a way that erodes employees' rights.

In October 2023, the Office of the Information and Privacy Commissioner of Ontario, the Office of the Information and Privacy Commissioner of British Columbia and the Office of the Privacy Commissioner of Canada co-sponsored a resolution at the Global Privacy Assembly on Artificial Intelligence and Employment. The resolution highlighted how AI, when "misapplied, incorrectly designed or inappropriately relied upon" may "lead to harms or infringement of fundamental rights and freedoms, including privacy, human dignity, equality of rights such as unfair discrimination." The resolution

emphasized the importance of ensuring the use of AI systems in an employment context is human-centric and that organizations comply with privacy laws when using AI. This includes ensuring fairness and transparency in processing personal data, and ensuring individuals have a right to access information about what data is held by an employee and how their personal data is used in connection with AI-assisted decisions.

Guidelines

If government institutions and local authorities are contemplating projects, programs or activities that involve employee personal information, they are required to do the following:

1) Identify the purpose for the collection, use and/or disclosure of employee personal information.
    a. This includes identifying the least amount of personal information that is necessary, reasonable, and required to achieve the purpose.
2) Identify the legal authority for the collection, use, and/or disclosure of employee personal information.
3) Establish policies and procedures that address the following:
    a. How employee personal information will be collected, used and/or disclosed.
        i. This includes exploring and identifying the least privacy-intrusive method of collecting, using and/or disclosing personal information.
    b. How employee personal information will be safeguarded.
    c. Who can access employee personal information and under what circumstance they can do so.
    d. Retention periods for employee personal information.
    e. How employee personal information will be disposed once the retention period is fulfilled.
    f. A process for responding to privacy questions and complaints from employees.
    g. A process for responding to access to information requests and correction requests under FOIP and LA FOIP.
    h. Establish governance and accountability mechanisms to ensure policies and procedures are being following. This includes setting internal checks and balances are in place to prevent the improper collection, use and/or disclosure of personal information beyond the identified purposes.
4) Provide training on the above policies and procedures to employees on an annual basis so that employees are aware of how their personal information is being collected, used and/or disclosed.
    a. Employees should be informed of electronic monitoring tools and AI systems being used and for which purposes.

b. Employees should be informed about how to object to the collection, use or disclosure of their personal information, how to challenge decisions made about them, and how to exercise their access rights.

A Privacy Impact Assessment (PIA) is a process that assists organizations in assessing whether a project, program or process complies with FOIP or LA FOIP. If personal information is involved in a proposed project, program or process, government institutions and local authorities should undertake the PIA process. For more information about PIAs, check out the office's PIA resources at the following links:

PIA Guidance Document: https://oipc.sk.ca/assets/privacy-impact-assessment-guidance-document.pdf

PIA Step 1 Preliminary Analysis worksheet: https://oipc.sk.ca/assets/pia-step-1-preliminary-analysis.docx

PIA Step 2 Define the Project worksheet: https://oipc.sk.ca/assets/pia-step-2-define-the-project.docx

PIA Step 3 Privacy Analysis worksheet: https://oipc.sk.ca/assets/pia-step-3-privacy-analysis.docx

PIA Step 4 PIA Report worksheet: https://oipc.sk.ca/assets/pia-step-4-pia-report.docx

In addition to a PIA, when considering the use of AI, organizations should consider conducting an algorithmic impact assessment to identify and mitigate risks to the rights of individuals and communities. An example of an algorithmic impact assessment is the Government of Canada's Algorithmic Impact Assessment tool. Organizations should seek information about the source of data used to train the AI system and assess whether the AI technology was developed in compliance with FOIP or LA FOIP.

Other Resources

Video Surveillance Guidelines for Public Bodies: https://oipc.sk.ca/assets/video-surveillance-guidelines-for-public-bodies.pdf

Protecting Employee Privacy in the Modern Workplace: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/joint-resolutions-with-provinces-and-territories/res_231005_02/

Contact Information

If you have any questions or concerns, please contact us:

306-787-8350 | toll free 1-877-748-2298
503 – 1801 Hamilton Street | Regina SK S4P 4B4
intake@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC