TECHNOLOGY'S IMPACT UPON EMPLOYEE PRIVACY

FEBRUARY 2018

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) provides 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.

The purpose of this document is to provide guidance to government institutions and local authorities on how they can 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 conducting employee monitoring activities, government institutions and local authorities must know the purpose for which they are collecting employee personal information. Then, individuals must be informed of the purpose prior to or at the time of the collection.

However, employee monitoring activities often occur as a result of "function creep". Function creep occurs when information is used for a purpose that is not the original 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 would be 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 they 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 GPS devices, radio-frequency identification (RFID) chips, and device identifiers such as the media access control (MAC) address and Internet Protocol (IP) address.

GPS

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 installing GPS devices into vehicles or tracking mobile devices.

RFID CHIPS

RFID chips with a unique serial number are often installed into employee badges. The RFID chips become activated when a RFID chip reader is nearby. Organizations can use RFID chips and RFID readers to track employees' 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

In order for organizations to manage and secure their IT systems, they will use software to monitor activities that are occurring on their network. However, such software can also be used for secondary purposes such as monitoring employee activity (personal Internet usage, recording key strokes, etc) to determine employee engagement and productivity.

Another method of tracking employee activity is the auditing capabilities of systems. Auditing features may record how employees have interacted with information stored within a system.

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 employees 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 their 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, an employee of the City of Saskatoon (a bus driver) alleged his privacy was breached when the City used footage of from its video surveillance 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 for organizations to 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.

GUIDELINES

If government institutions and local authorities are contemplating projects, programs, or activities that involves employee personal information, government institutions and local authorities should be prepared to do the following:

1) Identify the purpose for the collection, use, and/or disclosure of employee personal information,
2) The legal authority for the collection, use, and/or disclosure of employee personal information,
3) Have established policies and procedures that addresses the following:
    a. How employee personal information will be collected, used, and/or disclosed,
    b. How employee personal information will be safeguarded,
    c. Who can access employee personal information and under what circumstance they can do so,
    d. Establish retention periods for the employee personal information,
    e. How the 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.
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.

Government institutions and local authorities should undertake the Privacy Impact Assessment (PIA) process. A 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 my 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

OTHER RESOURCES

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

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 S4X 4H7

webmaster@oipc.sk.ca | www.oipc.sk.ca | @SaskIPC