Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

GUIDANCE DOCUMENT

EMPLOYEE PRIVACY RIGHTS

NOVEMBER 2017

CONTENTS

PURPOSE OF THIS GUIDANCE DOCUMENT

This guidance document discusses the privacy impacts of employee monitoring programs. Employees have a right to privacy in the workplace, which Canadian courts have upheld and must be respected by public and private organizations.

The *Personal Information Protection Act* (PIPA) sets out how private sector organizations can collect, use, and disclose personal information. More than 380,000 organizations in BC are subject to PIPA, including businesses and corporations, unions, political parties and not-for-profits. The *Freedom of Information and Protection of Privacy Act* (FIPPA) sets out how public sector organizations can collect, use, and disclose personal information and applies to 2,900 public bodies in BC.

Employee monitoring can include video and audio surveillance, software, and GPS tracking. Organizations may be tempted to use employee monitoring to provide safety coverage or for greater transparency. However, these tools can also unlawfully collect personal information about employees and ultimately increases risk.

EXAMPLES OF EMPLOYEE MONITORING

Video and Audio Surveillance

We have seen an increase in the presence of surveillance cameras in many parts of our lives. Whether we're catching the bus to work, filling a prescription, or shopping for groceries, video surveillance has become ubiquitous. The technology is increasingly inexpensive and easily accessible, and some organizations believe it can serve as a visual deterrent for criminal activity and inappropriate behaviour.

Surveillance systems are now appearing in the workplace, continuously collecting personal information of employees and customers. The threshold that private organizations must meet to use video surveillance on employees is high: it must be reasonable for the purpose of creating, managing or terminating an employment relationship. Continuous video surveillance is only reasonable when used as a last resort, after exploring other less privacy-invasive methods. For public bodies, the collection must be necessary for managing or terminating an employee relationship.

Audit and Compliance Report P16-01 looked at the use of video and audio surveillance in a private medical clinic. The clinic had surveillance cameras in its lobby, hallways, back exits and fitness room that captured the personal information of employees, customers and other individuals. The audit found the use of video surveillance in this case to be excessive – the clinic was not authorized to collect personal information through its video surveillance system.

Employers must carefully weigh the privacy harm when considering the use of video surveillance. A video camera cannot – and should not – replace adequate employee supervision.

For more information about video and audio surveillance, read
Audit and Compliance Report P16-01: Over-collected and Overexposed: Video Surveillance and Privacy Compliance in a Medical Clinic

Employee Monitoring Software

Employers have a need to combat internal and external threats to their information technology (IT) systems, such as malware, social engineering, and unauthorized access by employees. Software tools can provide some protection; however they can also lead to the over-collection of personal information about employees, through deliberate means (use of employee monitoring software) or inadvertent means (network firewalls that monitor website and email traffic).

Employers commonly allow employees to use workplace IT systems for some limited and appropriate personal use. Employers have a right to manage their IT networks for security and they may also ensure employees are not using excessive amounts of work time for personal reasons (checking social media accounts, online shopping, etc.). However, employers must notify employees of any monitoring that is implemented and the purpose for which the information is collected.

Investigation Report F15-01 examined the use of employee monitoring software by the District of Saanich. The District had installed software that captured keystroke logging, automated screen shots, and continuous tracking of computer program activity on employee workstations.

The Commissioner found under FIPPA that an employer can only collect personal information that is directly related to and necessary for the protection of IT systems and infrastructure. The collection of every keystroke and email – or screen captures of computing activities at 30-second intervals – clearly exceeded that purpose and was not authorized by privacy law.

That investigation report serves as a resource for both public bodies and private organizations subject to BC privacy laws.

> For more information about employee monitoring software, read
> ***Investigation Report F15-01: Use of Employee Monitoring Software by the District of Saanich***

GPS Tracking

New smartphone applications have made GPS tracking an easy way to monitor employees. By installing an app on an employee's phone, employers can track an employee's every movement. GPS tracking devices installed in employer owned vehicles can also include other monitoring and sensing technologies that can track and report more than just vehicle location, but also vehicle braking information, seat belt indicators and even driver behaviour.

Many privacy commissioner orders and court cases have confirmed that information gathered by an employer about an employee's location and behaviour using GPS and remote sensing is considered personal information, *not* solely information about the device or vehicle. It does not matter whether the device is personal or work-issued, what matters is that the employer is collecting the information about an employee.

Certain circumstances may allow the use of GPS to map employee travel routes, manage hours of work, and ensure that employees drive safely and lawfully. These may require the knowledge and consent of the employee prior to their implementation and use.

Orders from this office have determined that in most instances BC privacy laws do not allow continuous, real-time monitoring of employees outside of work hours by GPS tracking. Such pervasive tracking would most likely be considered excessive and invasive.

OIPC Order P12-01, Schindler Elevator Corporation (Schindler), looked at a company that used GPS and engine status data systems to record the location and behaviour of employees when performing work duties. The order resulted from a complaint from an employee that Schindler's collection of personal information via the tracking systems contravened PIPA.

The Commissioner determined that Schindler was authorized to collect the information in this case, as the purposes were to ensure employee safety, and to enable client billing. Because of

the unique arrangements, the company's employees were dispatched directly from their homes in work vehicles and infrequently attended at the employer's workplace.

This order emphasizes that context matters: if Schindler was using the technology to gather information outside of work hours, continuously, covertly, or for a different purpose, the collection of personal information would not be authorized under PIPA.

Similarly, in Order F13-04, the University of British Columbia was authorized to collect personal information from GPS systems installed in its campus security patrol vehicles in order dispatch patrol vehicles efficiently, locate patrolling employees for their safety, as those employees generally patrol alone.

For more information about GPS tracking, read
Order P12-01, Schindler Elevator Corporation and
Order F13-04, University of British Columbia

CONSENT

Are employers required to get an employee's consent before collecting personal information?

In the private sector, PIPA requires an organization to obtain consent before collecting personal information about an individual. However, it provides authority for the collection, use, and disclosure of employee personal information *without consent* if it is solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual.

While PIPA allows for this collection without consent, it requires that the employer notify the employee that it is occurring, and to explain the purpose(s) for the collection (such as employee safety).

In the public sector, FIPPA does not require consent for the collection of personal information from employees. It allows such collection where it is necessary for and directly related to a program or activity of the public body.

For example, in the UBC order mentioned above, the Commissioner agreed with UBC that GPS surveillance was necessary for employee safety purposes, patrol dispatch efficiency and maintenance purposes, and that those purposes were directly related to a UBC program or activity.

However, FIPPA does require a public body to notify an employee that it will be collecting personal information for the purposes of managing or terminating an employee relationship, if that information is indirectly collected.

PRIVACY MANAGEMENT PROGRAM

Section 5(a) of PIPA requires organizations to develop and follow policy and practices that are necessary for the organization to meet its PIPA obligations. Accountable privacy management begins with an appropriate framework and supporting policies and programs to ensure adequate protection of personal information in an organization's custody or under their control.

Privacy policies should address the following, at a minimum:

- The purposes for collection, use and disclosure of personal information, including requirements for consent and notification;
- Access to and correction of personal information;
- Retention and disposal of personal information;
- Responsible use of information and information technology, including administrative, physical and technological controls and appropriate access controls; and
- A process for responding to privacy complaints.

The best way for an organization to demonstrate compliance with BC privacy law is to implement a privacy management program. The principal elements of a privacy management program should include:

- Adequate resources for the development, implementation and monitoring of privacy controls;
- The presence of applicable policies and procedures;
- Up-to-date documentation of risk assessment and mitigation strategies;
- Adequate training delivered regularly;
- Adequate information incident management processes;
- Compliance monitoring; and
- Regular reporting to the executive.

When organizations process a relatively small amount of personal information, such as the personal information of a handful of employees only, then the privacy management program should be appropriately tailored to the structure, scale, volume, and sensitivity of those personal information processing activities.

For example, a person responsible for ensuring that their organization is compliant with privacy law may also carry a range of other responsibilities with the company.

However, a company that has extensive information processing activities involving the collection of sensitive personal information may requiere a dedicated privacy officer. The privacy officer is accountable for managing how the organization processes personal information.

Instituting a video and audio surveillance program, for example, would significantly increase the personal information processing activities of any organization, and the organization's privacy management program should be scaled appropriately.

One of the key components of a privacy management program is undertaking a privacy impact assessment (PIA) before introducing a new privacy invasive technology into the workplace. PIAs assist organizations in introducing new policies or programs that involve personal information.

ADVICE FROM THE COMMISSIONER	An assessment should be completed **prior** to implementing an employee monitoring program, where the appropriate authority to collect the information would be identified.

ADDITIONAL RESOURCES

- Guide to using overt video surveillance
- Mobile devices: Tips for security & privacy
- IT security and employee privacy: Tips and guidance
- Guidance for the use of body-worn cameras by law enforcement authorities
- Public sector surveillance guidelines
- Getting accountability right with a privacy management program
- Accountable Privacy Management in BC's Public Sector
- A guide to PIPA for businesses and organizations
- Investigation Report F15-01: Use of employee monitoring software by the District of Saanich
- Audit and Compliance Report P16-01: Over-collected and overexposed
- Order P12-01: Schindler Elevator Corporation
- Order F13-04, University of British Columbia

Office of the
Information &
Privacy Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 | Toll free in BC: 1-800-663-7867 info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy