

# Employee Surveillance: What's "Reasonable"?



A recent decision from the British Columbia Privacy Commissioner should remind employers that simply having a valid purpose for the collection and use of employee personal information does not necessarily mean it was reasonable to do it.

In *Teck Coal Limited (Re)*, several employees filed a complaint with the commissioner that their employer was collecting and using employee personal information contrary to British Columbia's *Personal Information Protection Act*. Specifically, they complained the employer's use of several surveillance cameras located in the facility contrary to *PIPA*.

The background facts are not particularly complicated. The employer ran a mining operation. They installed cameras to monitor a "tool crib" and hallway in the facility. These cameras operated 24/7 and saved recordings to a server for a period of 30 days before deletion. The footage could be viewed live, or accessed by individuals with appropriate clearance.

Adjudicator Syrotuck first concluded that video records of employees fit the definition of "employee personal information" (EPI). *PIPA* generally allows the use and collection of EPI without consent as long as the employer complied with *PIPA*.

*PIPA* defined EPI as:

personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment;

The adjudicator agreed that the employer was collecting and using personal information solely for the purposes of preventing and investigating employee theft and for monitoring operations. She accepted that the **purpose** of the collection and use was to manage the employment relationship. She was satisfied that the personal information in question was "employee personal information" as defined.

In order to use and collect EPI without employee consent, the employer was

required to comply with sections 13 and 16 of *PIPA*. The employer argued that 13(2)(a) and (b) applied, as well as 16(2)(a) and (b). The bulk of the decision focused on (2)(b) of each section.

Section 13 addressed the **collection** of EPI:

- 13 (1) Subject to subsection (2), an organization may **collect** employee personal information without the consent of the individual.
- (2) An organization may not collect employee personal information without the consent of the individual unless
- (a) section 12 allows the collection of the employee personal information without consent, or **(b) the collection is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual. [emphasis added]**
- (3) An organization must notify an individual that it will be collecting employee personal information about the individual and the purposes for the collection before the organization collects the employee personal information without the consent of the individual.
- (4) Subsection (3) does not apply to employee personal information if section 12 allows it to be collected without the consent of the individual.

Section 16 addressed the **use** of EPI:

- 16 (1) Subject to subsection (2), an organization may **use** employee personal information without the consent of the individual.
- (2) An organization may not use employee personal information without the consent of the individual unless
- (a) section 15 allows the use of the employee personal information without consent, or **(b) the use is reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual. [emphasis added]**
- (3) An organization must notify an individual that it will be using employee personal information about the individual and the purposes for the use before the organization uses the employee personal information without the consent of the individual.
- (4) Subsection (3) does not apply to employee personal information if section 15 allows it to be used without the consent of the individual.

In arguing that s. 13(2)(b) and 16(2)(b) applied, the employer stated it used the EPI gathered by the cameras for three main purposes: allowing supervisors to check the status of production and the safety of work/theft, occasional downloading to review safety or production incidents, and assist human resources if an employee is facing disciplinary consequences. In contrast, the employees advised that the surveillance invaded their privacy and dignity by creating a sense of constant observation.

While the adjudicator acknowledged that the *purpose* of the collection and use of EPI was reasonable, the primary question was whether the use and collection itself was reasonable. She identified the following factors for an adjudicator to consider:

1. sensitivity of the employee personal information (*i.e.*, health history or a medical condition is sensitive information, but an employee's name or home address is not);
2. amount of personal information (*i.e.*, Is the employer collecting, using or disclosing more information than is necessary to achieve its purpose(s)?);
3. likelihood of effectiveness (*i.e.*, Is there a reasonable likelihood that the collection, use or disclosure of personal information will fulfil the employer's objectives?);
4. manner of collection and use of the personal information (*i.e.*, Was the employee aware that the information was being collected, or was it covertly collected? In what circumstances and how often does the employer access the information?);

5. less privacy-intrusive alternatives (*i.e.*, Has the employer given reasonable consideration to other methods for achieving its objectives? This factor does not necessarily require the employer to implement the least privacy-intrusive alternative, but the employer must consider the balance between its interest and the right of individuals to protect their personal information); and
6. other relevant factors given the circumstances.

Ultimately, the adjudicator concluded that the employer could not establish the collection and use was reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual. Despite finding that the information was not particularly sensitive and the surveillance was not "covert", she concluded that the employer's failure to provide evidence of past effectiveness, combined with the 24/7 recording rendered the surveillance unreasonable. However, she did find that surveillance that took place *after* work hours would be reasonable.

She also noted that while signage was posted through the facility that there was surveillance in place, she found the lack of signage specifying exactly which buildings had cameras was insufficient notice under section 13(3) and 16(3).

Ultimately, the adjudicator ordered the employer to cease collecting and using information from the tool crib cameras, and to cease collecting and using information from the office cameras during work hours.

## **The Take Away**

This decision demonstrates the difficulties employers can have when attempting to balance their operational and workforce management needs with legislative privacy requirements. It is also somewhat ironic that the adjudicator considered the lack of past incidents demonstrative of a lack of effectiveness. When assessing proper risk controls and treatment, physical systems like surveillance cameras are considered effective tools in managing risk. Not only do they allow for subsequent investigation, they also serve as a deterrent. One could argue (and the employer probably did) that the lack of past examples actually proves their effectiveness.

With privacy legislation varying from province to province in Canada, employers with operations in multiple jurisdictions will need to ensure that their local practices comply with local acts. As an example, Ontario does not have its own general application privacy legislation that addresses employee personal information. Although the federal *Personal Information Protection and Electronic Documents Act*, would apply to a private employer, its protection of "employee personal information" is limited to those employers that are federally regulated. For most other Ontario employers, there are no specific legislated privacy rights regarding employee personal information. While employees have common law rights to privacy, the extent of these rights can vary based on the nature of the employer. An employer may also be able to vary the reasonable expectation of privacy by contractual terms within the contract of employment. Whether a certain method of risk control is appropriate will be a case by case assessment. Ultimately, it will come down to what is "reasonable" in the circumstances, which we can see is never clear-cut.

See *Teck Coal Limited (Re)*, 2020 BCIPC 24 (CanLII)

*The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.*

by Devan Marr, Strigberger Brown Armstrong LLP