

Do Workplace Surveillance Cameras Violate Employees' Privacy Rights?



Employers have a legitimate interest in using surveillance cameras, drones, artificial intelligence (AI) sensors, and other technologies to maintain workplace safety and security. However, the employee images and data that monitoring solutions capture are also deemed personal information protected by the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial privacy laws. This scenario, which is based on an Ontario case, is an excellent illustration of where the lines are drawn.

Situation

After a series of thefts and acts of vandalism, a railway installs six video surveillance cameras in its maintenance yards. Although used mostly to monitor comings and goings of the public, the cameras also capture some employee activity. The railway posts signs at entrances warning of the cameras. It tells employees that the cameras are the only feasible way to protect security and reassures them that it won't use the footage to monitor productivity or impose discipline. In fact, the cameras aren't monitored but used only to investigate incidents. Employees claim that the cameras are an invasion of privacy and demand their removal.

Question

Does the railway have a right to keep the surveillance cameras installed?

1. No, because the railway didn't get employees consent to install the cameras.
2. Yes, because the cameras are necessary and used only for security purposes.
3. No, because the cameras record employee activity, which is protected personal information.
4. Yes, because it owns the property and can place surveillance cameras wherever it wants.

Answer

1. The railway can keep the cameras because they're necessary to serve a legitimate security purpose.

Explanation

The Ontario court ruled that the cameras could stay because:

- The railway notified employees about them (monitoring is harder to justify when it's surreptitious).
- The cameras were used principally to monitor visitors for security rather than employees for productivity or disciplinary purposes.
- Footage was accessible only to "responsible management" and the police in response to actual incidents.
- The cameras were placed in public areas where expectation of privacy was minimal.
- Less privacy-invasive alternatives such as fencing or security guards were ineffective and infeasible.

[*Eastmond v. Canadian Pacific Railway*](#), 2004 FC 852 (CanLII)

Why Wrong Answers Are Wrong

A is wrong because privacy laws allow for using, collecting, and disclosing personal information without consent for limited, legitimate purposes, such as deterring theft or vandalism or protecting security and safety.

C is wrong because it's okay to collect personal information, including tapes of employee activity, if, as in this case, it serves legitimate purposes, less privacy-invasive alternatives aren't feasible, and the use, collection, and disclosure of personal information is limited to the minimum amount necessary to accomplish the legitimate purpose.

D is wrong because courts, arbitrators, and privacy tribunals have repeatedly found that PIPEDA and other privacy laws ban employers from installing video cameras or other privacy-invasive monitoring technology on their own property for disciplinary purposes or to monitor employee productivity.