Avoid Privacy Violations When Using GPS and Other Monitoring Technologies for Safety

Digitally monitoring employees can get you into trouble even if you're just trying to ensure safety.

Use of GPS, cell phone and other digital technologies to monitor workers' activities and whereabouts can go a long way in ensuring health and safety, especially true for staff who telecommute or work alone or at an offsite location. But it can also get you into hot water, especially if you're in Ontario. Here are the compliance risks and how to manage them.

The Legal Risks of Digitally Monitoring Employees

Use of digital monitoring solutions may violate employees' privacy rights under the following laws:

PIPEDA & Provincial Privacy Laws

Personal privacy legislation, including the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), which applies in all parts of the country, limit the collection, use and disclosure of protected personal information. However, PIPEDA applies to "commercial activities," not workplaces, other than in federally regulated workplaces and the 3 territories. Meanwhile, BC, Alberta and Québec have adopted their own provincial laws that do give employees personal privacy rights vis-à-vis their employers.

Ontario Bill 88

Ontario recently enacted new legislation, Bill 88, the Working for Workers' Act, 2022, that doesn't ban but does restrict employer use of electronic monitoring technology. Specifically, the legislation requires employers to adopt a written policy telling employees that they're being monitored, as we'll explain below.

Common Law Privacy Rights

Workers may also have personal privacy rights, aka, reasonable expectations of privacy, under what's called "common law," or non-statutory law that comes from court

cases. The leading case is a 2012 ruling called *Jones v. Tsige*, (2012 ONCA 32 (CanLII)), in which the highest court of Ontario recognized a new privacy tort called "intrusion upon seclusion" and awarded a bank employee $10,000. To make out a case, workers must show not simply that the employer invaded their privacy, but that the conduct was intentional or reckless and such that a reasonable person would consider highly offensive and causing distress, humiliation or anguish.

Contractual Privacy Rights

Employees may also have reasonable expectations of privacy under their collective agreement or employment contract. **Example:** A food plant installed surveillance cameras to monitor who entered and exited, prevent theft and trace sources of food contamination. The union contended that use of the surveillance cameras violated employees' privacy rights under the collective agreement. After balancing the employer's interest in security and food safety against the employees' privacy expectations, the Ontario arbitrator ordered the employer to remove the cameras in the food production areas while allowing it to keep the cameras at the entry and shipping areas [*United Food & Commercial Workers Union, Local 100A v. James Family Foods,* [2006] CanLII 36615 (ON L.A.)].

4 Ways to Keep Monitoring Solutions Privacy-Compliant

Based on court, arbitrator and privacy commission rulings on use of video surveillance in the workplace, there are 4 things you can do to manage privacy risks of digitally monitoring your employees:

1. Limit Use to Safety Purposes

Rule of Thumb: While all agree that safety, as opposed to ensuring productivity, is a reasonable and appropriate purpose for use of monitoring technology, employers must still show that:

- The use of the technology is "demonstrably necessary" to meet the safety need;
- The technology is likely to be effective in meeting that need;
- The loss of employees privacy is proportional to the benefit gained; and
- There are no less privacy-invasive ways of achieving the purpose.

2. Keep Information Collected to a Minimum

Collection must be limited only to personal information necessary to accomplish the purpose of deploying the technology and not include non-work-related personal information in which employees have reasonable expectations of privacy. Accordingly, software or apps that tap into employees' personal calls, emails or computers are highly problematic, as is spyware and other technologies for secretly monitoring employees without their knowledge.

3. Consider Need for Consent

You generally need consent to collect, use or disclose employees' personal information unless:

- Getting consent would compromise the availability or accuracy of the information collected; and
- Collecting information is for the purpose of investigating violations of the law or employment agreement.

4. Create Written Policy Disclosing Use of Monitoring Technology

Remote monitoring technology is more privacy-invasive when you use it surreptitiously without employees' knowledge. That's why you should let employees know they're being monitored. One option is following the Bill 88 approach. Under Bill 88, Ontario employers have until January 1, 2023, to adopt a written policy describing:

- The electronic monitoring devices they use;
- The information those devices collect; and
- How the company uses the information it collects; and
- The third parties to which it discloses that information.

Employers with 25 or more employees must also disclose the purposes of using such devices.