How to Use Technology Legally to Track Workers for Safety

Although most workers work in workplaces filled with co-workers, many work by themselves. Some work after hours, such as security guards or cleaning staff, while others work offsite, such as salesmen, couriers and repair technicians. Such workers are vulnerable because they may not be able to get help if something happens, such as they get injured, stranded or attacked. As a result, employers have a duty to take steps to ensure the safety of workers when they're alone. To fulfill that duty, can employers use technology such as GPS to track workers on their own? The simple answer is yes—provided you meet certain requirements under the privacy laws. Here's a look at the interplay between the OHS and privacy laws, some cases on this issue and five requirements you need to understand.

OHS DUTIES V. PRIVACY

Tracking workers working alone for their safety implicates two types of laws:

OHS laws. The OHS laws in most jurisdictions specifically require employers to take steps to protect workers who work alone. "Working alone" is typically defined as meaning that the worker is the only worker at that workplace in circumstances where assistance isn't readily available to the worker in case of injury, sickness or other emergency. In the jurisdictions without specific working alone requirements, the duty to protect workers working alone is implied under the general duty clause of the jurisdiction's OHS act.

The use of technology is a critical component in fulfilling working alone duties. For example, the OHS laws typically require employers to set up communications systems for workers working alone, such as by providing them with cell phones, satellite phones or panic buttons.

Privacy laws. Although tracking workers may be a useful way to comply with employer duties under the OHS laws, it can run afoul of the privacy laws, which limit the gathering and use of personal information on workers. The key personal privacy law is *Personal Information Protection and Electronic Documents Act (PIPEDA), a federal law.*

PIPEDA applies to all organizations engaged in commercial activities unless the federal government exempts an organization or activity in a province that has a law substantially similar to PIPEDA. The only provinces to date with privacy laws deemed

substantially similar to PIPEDA are AB, BC and QC. (Several other jurisdictions have privacy laws that apply to workers' health information only.)

In general, federal and provincial privacy laws protect individuals from the use and disclosure of their personal information without their consent, except as otherwise permitted by law. An employer can collect so-called "employee personal information" if it gives workers notice about the purpose for collecting and using such information. In addition, the employer's collection and use of the information must be reasonable for establishing, managing or terminating an employment relationship.

SAFETY V. PRIVACY CASES

Several cases have been decided on the impact of personal privacy laws on the use of technology for workers' safety. Most have been decided by Privacy Commissioners, who oversee compliance with the privacy laws in their respective jurisdictions.

Example: An employer collected GPS and engine use data from employer-owned vehicles its mechanics used to service and repair clients' elevators. The drivers claimed the information collection violated their privacy rights. The employer had various reasons for collecting this information, including safety. It cited one example where concerned co-workers couldn't find an employee and the system allowed it to track down this employee. The employer also said the system helped with an investigation into a workplace fatality involving a mechanic.

The Information and Privacy Commissioner of BC determined that the data on the vehicles driven by the mechanics was protected employee personal information. However, the employer provided notice regarding the information's collection and use. And its collection and use of the information were tailored to the intended purpose—which included to ensure drivers' safety—were likely to be effective, didn't involve sensitive information and didn't harm the mechanics' dignity. Finally, the Commissioner found there were no other suitable alternatives [*Order P12-01, Schindler Elevator Corp (Re)*].

Here are some other examples in which employers won:

- An elevator service company was permitted to collect information from the GPS in the cell phones its mechanics used while they were on duty because it didn't collect more information than was necessary; the system was likely to be effective; the collection and use of the GPS information wasn't an offence to the mechanics' dignity; and the company had provided adequate prior notice of its intent to collect this information [*Kone Inc (Re)*].
- A telecommunications company installed GPS receivers in its work vehicles, which captured vehicle stop and start times, speed, location, mileage and off-shift parking location. Workers complained to the Office of the Privacy Commissioner of Canada that the company was improperly collecting their personal information—that is, their daily movements while on the job—without their consent. The Commissioner approved the company's use of GPS to collect the information for safety, dispatching and asset management and protection purposes. But she also ruled that the use of GPS to manage and evaluate workers' performance was only appropriate in "certain limited, exceptional, and defined circumstances" [*PIPEDA Case Summary #351*].

But employers' tracking of workers isn't always upheld.

Example: A university gathered GPS information from its on-campus security patrol vehicles to monitor the whereabouts and behaviour of security guards on duty. The university installed the equipment so it could, among other things, locate security

guards for their safety. The union challenged the collection on privacy grounds.

The Information and Privacy Commissioner of BC ruled that the information collection wasn't permissible. The information collected from the patrol vehicles was personal information under privacy law. But the university's monitoring activities and information collection were directly related to campus security, including employee safety; guards weren't continuously monitored; and the information collected from the GPS system wasn't sensitive. However, the Commissioner also found that the university's privacy policy was inadequate. For example, it was unclear as to how the university would use the information collected. And the university didn't give guards notice of its intended purposes for implementing the GPS system and collecting and using information from it until *18 months after* it began collecting personal information. So the Commissioner ordered it to stop collecting, using or disclosing personal information from the GPS system until it complied with the notice requirements [*University of British Columbia (Re)*].

5 TRACKING REQUIREMENTS

If you intend to use technology, such as GPS, to track workers when they're alone and collect information on their whereabouts and movements, the cases have firmly established that such information is protected by the personal privacy laws. But the cases also demonstrate that you can collect this personal information provided that you comply with these five requirements:

1. Consider less intrusive alternatives first.

Tracking workers and gathering information on where they go, how long they stay there, what routes they take, etc. is an invasion of their privacy. In fact, it essentially sounds like stalking. So the cases have held that employers wouldn't be able to collect such private information if there's another viable and less intrusive alternative. For example, it's unlikely an employer would be allowed to track the GPS in janitorial workers' cell phones if they're working in one fixed location and other alternatives are available to adequately protect them, such as requiring them to check-in on a regular basis.

2. Choose a system that's likely to be effective.

The system you choose to use to track workers must be effective for the purposes you want to implement it, that it, to ensure their safety while they're working alone. For example, a system that downloads information from GPS installed in a truck only once a month won't help you locate the driver if he goes missing. You essentially need real-time access to this information for it to be effective for safety purposes.

***Insider* Says:** Safety isn't the only reason you may be able to collect workers' personal information. In fact, you may want to collect such information for multiple reasons. PIPEDA permits the collection of workers' personal information without their consent if it's "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual." So you may also be able to collect GPS information for company trucks, say, to determine the most efficient routes for drivers to take. And a system that only downloads the data once a month might be effective for that purpose.

3. Don't collect more information than necessary.

You can only collect the information you need to ensure worker safety. If you collect additional, unnecessary private information, your system may not survive a challenge. In other words, collecting GPS information from workers cell phones is one thing;

collecting information on who they text, what websites they access or apps they use is another altogether.

Timing is also an important element here. While you may be permitted to track workers while they're on duty, you can't do so when they're not working. So if workers are permitted to drive their company cars or use their company phones off duty, your system must have a way of distinguishing between when workers are on the clock and when they're not. For example, in the *Kone* case, the system was designed not to collect information from mechanics' phones when they were at lunch, attending personal appointments during the work day or off duty.

4. Exercise care when using information to mange workers.

The use of technology can't offend workers' dignity. This issue usually arises in the context of concerns that the information gathered would be used to evaluate workers' performance, such as by determining how fast they're driving or if they're where they're supposed to be during the work day, and even impose discipline. Privacy commissioners will generally allow the information gathered from tracking technology to be used for worker management provided that the employer doesn't rely solely on such information or assumptions based on it. For example, you shouldn't suspend a worker just because the GPS in his car indicates that he wasn't at a particular client's location when he was scheduled to be there without further investigation. By bringing the information to the worker's attention and asking him about it, you may learn that, say, the client called the worker directly and rescheduled the appointment, so the worker took his lunch break early. However, it *is* appropriate to use the gathered personal information to verify issues raised independently, such as a complaint that a truck driver was speeding.

In addition, if you plan to use the personal information gathered for employee management, you must make such purposes clear to workers and establish a policy spelling out the situations in which you'll use this information for performance management and outlining an appropriate process of warnings and progressive monitoring. For example, your policy may state that you'll use the personal information to investigate a complaint from a member of the public, investigate concerns raised internally or address productivity issues. It's also important to train all managers and supervisors to ensure that they use the personal information collected appropriately.

5. Provide adequate prior notice of intent to collect this information.

It's critical that you notify workers that you intend to collect certain personal information about them *before* you actually implement the system. Remember the *University of BC* case mentioned above—the employer's efforts to collect information on campus guards' movements failed primarily because it didn't satisfy the notice requirements.

The privacy laws generally require employers to provide specific, meaningful notice so workers know:

- Personal information is going to be collected;
- What types of information are going being collected;
- How the information will be collected;
- Why you're collecting the information, that is, the purposes for the collection; and
- How you'll use this information.

You can provide such notice in written policies or memos to workers and through

training sessions on the policy. For example, in the *Kone* case, the company used detailed PowerPoint presentations containing a significant amount of information on its collection and use of information from the mechanics' cell phones.

BOTTOM LINE

Technology can be very useful in ensuring worker safety, especially for workers who work outside the workplace. But even if you're using this technology with the best of intentions, workers may still object to tracking their movements or whereabouts. By complying with the requirements discussed above, you can strike the appropriate balance between worker safety and worker privacy.

SHOW YOUR LAWYER

***Kone Inc (Re)*, [2013] BCIPC 23 (CanLII), Aug. 28, 2013**

***Order P12-01, Schindler Elevator Corp (Re)*, [2012] B.C.I.C.P. No. 25, Dec. 19, 2012**

***PIPEDA Case Summary #351*, Office of the Privacy Commissioner, Nov. 30, 2006**

***University of British Columbia (Re)*, [2013] BCIPC 4 (CanLII), Feb. 1, 2013**