Avoid Privacy Pitfalls When Remotely Monitoring Telecommuter Productivity

You can track their productivity but you can’t spy on employees who work from home.

Before the pandemic, 82% of Canadian employees worked primarily from an external workplace; today, only 27% do. Coaxing employees to return to the workplace will be an uphill battle, with recent surveys suggesting that more than 9 in 10 of those who are currently working remotely want to continue spending at least some of their working hours at home. In short, employers need to adjust to the realities of telecommuting. Among the biggest challenges will be maintaining productivity. One potential solution is to deploy technologies that monitor employees’ whereabouts and use of computer and other work equipment to verify that employees who work remotely are actually doing their jobs. Unfortunately, doing this exposes you to liability risks under privacy laws. Here’s a look at the risks and how to manage them.

Remote Monitoring & Teleworker Productivity

Remote monitoring technology may include apps that employees upload onto their personal computers and network software that can monitor the network, internet, and email usage of a large group of employees to collect data showing when they’re idle, how often they surf the internet, how and how often they email and make phone calls, etc.

In addition to helping maintain telework productivity, these solutions enable organizations to protect confidential business information and keep work hour, overtime and other records required by employment standards laws.

Remote Monitoring & Telecommuter Privacy

Employers need to be aware that use of remote monitoring solutions may run afoul of employees’ privacy rights under the following laws.

PIPEDA and 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.

Common Law & Contractual Privacy Rights

Even so, telecommuters may have personal privacy rights, aka, reasonable expectations of privacy, under other laws, including in the 7 jurisdictions without PIPEDA workplace protections or provincial equivalents.

Common Law: The principal source of these rights is “common law,” or non-statutory law made by judges in deciding 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.

Routine use of remote monitoring solutions to manage telecommuters probably wouldn’t constitute intrusion upon seclusion. To rise to that level, the privacy violation would have to be pretty flagrant. Specifically, the telecommuter being monitored would have to prove that:

- The employer invaded the employee’s privacy;
- The conduct was intentional or reckless; and
- A reasonable person would consider the invasion highly offensive and causing distress, humiliation or anguish.

Contract Law: Telecommuters may also have reasonable expectations of privacy under their collective agreement or individual employment contract. Although there haven’t yet been any cases involving telecommuting monitoring, there’s been plenty of litigation finding that employer use of surveillance technology in the workplace crossed the line.

Example: A food company installed surveillance cameras in its factory to monitor who entered and exited the plant, trace sources of food contamination and prevent theft. The union contended that use of the surveillance cameras was unreasonable and 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 in place [*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

If your organization uses or is thinking about using technology to monitor employees who work remotely, you need to ensure that you do so in a way that doesn’t get you into trouble under privacy laws. The problem is that this is a new area of the law and we don’t have any cases or official guidelines specifically addressing how to do that. But what we do have is indirect guidance in the form of the clear rules that courts, arbitrators and privacy commissions use to evaluate the legality of cameras and other workplace surveillance technology.

1. Use Must Be Reasonable

Rule of Thumb: Employers can collect, use and disclose personal information only for purposes that a reasonable person would consider appropriate under the circumstances. Courts use a 4-part test to determine whether use of surveillance technology is reasonable and appropriate:

- The use of the technology must be demonstrably necessary to meet a specific need;
- The technology must be likely to be effective in meeting that need;
- The loss of privacy to the employees being monitored must be proportional to the benefit gained; and
- There must be no less privacy-invasive way of achieving the same end.

We know from surveillance technology cases, that courts are more open to use of privacy-invasive technology in the workplace when it's used for health, safety and security purposes.

Example #1: The Privacy Commissioner of Canada concluded that a locomotive company's use of surveillance cameras to safeguard employees' health and safety after a number of safety incidents was reasonable [*PIPEDA Case Summary #264*, 2004].

Example #2: The Alberta Information and Privacy Commissioner found it reasonable for an employer to install a GPS in employees' vehicles to promote safe driving and ensure compliance with OHS laws [*Nal Resources Management Ltd (Re*), 2019 CanLII 64575 (AB OIPC)].

Employers do, in fact, have responsibilities to protect telecommuters under OHS laws, at least in most provinces. And while remote monitoring solutions can serve those purposes, their primary purpose is to monitor telecommuter **performance or productivity.** Historically, courts have been reluctant to allow employers to install cameras, GPS and other privacy-invasive surveillance solutions for such purposes.

Example #1: Alberta Commissioner rules that oilfield maintenance service company's use of surveillance cameras to manage employee performance is unreasonable [*R.J. Hoffman Holdings Ltd*. (2005)]. the

Example #2: Privacy Commissioner of Canada concludes that internet service provider's use of surveillance cameras to manage the productivity of its sales, marketing and technical support staff is unreasonable because there were less privacy-invasive alternatives available [*PIPEDA Case Summary #279*].

It remains to be seen whether the prevalence of telecommuting will cause courts to loosen up and give employers more leeway to perform monitoring for productivity purposes.

2. Information Collected Must Be Kept to Minimum

Another key factor is what and how much personal information the employer collects to monitor telecommuters remotely. Collection must be limited only to the information necessary to accomplish the purpose of deploying the technology and not include non-work-related personal information in which telecommuters have reasonable expectations of privacy. Accordingly, software or apps that tap

into employees' personal calls, emails or computer use will be highly problematic.

Courts will also consider the kind of technology used. Spyware and technologies that enable employers to intercept communications, scan or capture images for content, monitor keystrokes or covertly listen into phone calls are particularly invasive and likely to raise privacy red flags.

3. Telecommuters May Need to Consent

Employers generally need consent to collect, use or disclose employees' personal information. But there are exceptions. As with surveillance cameras, the 2 exceptions most likely to justify use of remote monitoring technology without employee consent include:

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

Of course, exceptions are unnecessary when employees give their consent freely. This might be the situation with remote work to the extent that employers are in the position to require employees to consent to being tracked in exchange for being allowed to telecommute. Such consent would probably be legally valid, provided that it clearly spells out what information will be collected and how it will be collected and used.

4. Telecommuters Must Know They're Being Monitored

Remote monitoring technology is more privacy-invasive when you use it surreptitiously without employees' knowledge. For example, in a 2005 case, the Alberta Privacy Commissioner ruled against an employer that secretly installed keystroke logging software on an employee's work computer to monitor productivity. Information allowing an employer to know how employees use their work time may be necessary for employee management, the Commissioner reasoned. However, the keystroke software overreached and collected unnecessary information for employee management purposes.

Create a Written Telecommuter Monitoring Policy

The best way to manage privacy liability risk is to include specific language in your telecommuting policies and arrangements that provides for monitoring. The idea is to let employees know exactly what you're going to do and how and ensure they don't have reasonable expectations in the information collected. Like the template on the HRI website, your policy language should, at a minimum:

- Explain the purposes for which you use remote monitoring solutions;
- Describe the actual solutions you use and how they work;
- List the specific kinds of information to be collected, which should correspond to the attendance, performance and productivity standards that you'll use the data to monitor;
- Indicate who will have access to the information and how they'll use it;
- Require employees to accept and consent to these terms in exchange for being allowed to telecommute;

- List a contact person or office where employees can direct their questions or concerns; and
- Provide for accommodations to the policy.