

How, and when, employers should monitor employees

5 areas of law relate to workplace monitoring

BY ADRIAN MIEDEMA
AND ANDY PUSHALIK

Is it human nature to desire privacy or notoriety or both? It's hard to know, with YouTube celebrities, tell-all blogs and reality television on the one hand, and people clamouring for privacy on the other hand.

People seem to want to put the most sensitive and embarrassing details of their lives on public display, but then cry out about the importance of privacy. Perhaps what people really want is the freedom to choose.

As such, employees will not take kindly to employer monitoring forced on them without their consultation or consent. The workplace, however, is not a free country when it comes to privacy.

One Alberta judge said recently: "The workplace is not an employee's home and employees have no reasonable expectation of privacy in their workplace computers. It, therefore, follows that while employers may permit employees limited personal use of workplace computers, the employer is entitled to restrict the terms and conditions on which that use may be permitted."

There are a number or reasons why employers might monitor employees. They include information security, fraud prevention, prevention of criminal use of computers, investigation of misconduct and productivity assessment.

Various employee monitoring techniques are popping up in workplaces across Canada. They include the more common and prosaic security cameras, as well as monitoring of employee's email and Internet use and GPS tracking of vehicles. Other types of monitoring include network forensic software (which lets employers track and play back exactly what happens on employees' computer screens), iris or hand scanners (used instead of punch cards) and oral fluid swabs (used for drug testing).

There are essentially five areas of law relating to workplace monitoring:

privacy, labour relations, human rights, evidence admissibility and criminal law.

Privacy

At present, only employers in British Columbia, Alberta, Quebec and the federal jurisdiction are subject to private sector privacy laws in relation to personal employee information. These employers cannot collect, use or disclose personal employee information where a reasonable person would consider it inappropriate to do so. This "reasonableness" test places a critical restriction on the monitoring employers can do in those jurisdictions.

For example, an Alberta employer, concerned an employee was working too slowly, installed keystroke-logging software on his computer without telling the employee. The software logged every keystroke the employee made. But, in 2005, the Privacy Commissioner of Alberta disapproved of the keystroke monitoring and found it "highly intrusive."

In other cases, the federal privacy commissioner said a "voice print" password system — that provided employees with access to business applications — was acceptable if the employee consented to give a voice print, and while an employer was permitted to install a GPS system to track drivers' locations, it was not permissible to use the GPS data to evaluate the drivers (as doing so infringed on their privacy).

Also, a labour arbitrator found a company was entitled to introduce a hand scanner system instead of punch clocks where the system converted the hand scan to a numerical template and did not keep an actual handprint.

Labour relations

Union arbitration case law says unionized employers are not permitted to impose disciplinary policies — or policies that can result in discipline — unless they are reasonable.

In an arbitration decision involving Imperial Oil, the company was

not permitted to introduce oral fluid testing (which evidence showed could demonstrate whether an employee was impaired by drugs). The arbitrator stated the oral fluid test interfered with an employee's privacy and dignity and, therefore, any introduction of such testing is an "extraordinary measure" that can "only be resorted to where justification is established." Employers with unionized employees, therefore, have significant restrictions when monitoring employees.

Human rights

While human rights laws do not specifically deal with monitoring of employees, monitoring can uncover information relating to prohibited grounds of discrimination. For instance, monitoring of an employee's emails or Internet use can reveal her religion, marital status, family status or country of origin. Employers that monitor emails or Internet use should be aware an employee who is disciplined or discharged because of such monitoring may claim the real reason for the discipline or discharge was religion, race or another prohibited ground, which the employer learned about because of the monitoring.

Evidence admissibility

Judges do not like evidence that is obtained surreptitiously. In a worst-case scenario, a judge or adjudicator can refuse to admit or hear evidence derived from surreptitious monitoring or surveillance. Even if that evidence is admitted, it might not be given much weight. A well-crafted policy, that clearly puts employees on notice they will be monitored, can increase the probability a judge or adjudicator will admit and rely on monitoring evidence.

Criminal Code

Section 184(1) of the Criminal Code makes it a criminal offence to intercept a private communication using any "electro-magnetic" or other device. However, it is not an offence if the originator or recipient of the communication consents. Therefore, in order for employers to monitor employees' private emails, it is strongly recommended the employ-

TIPS FOR EMPLOYERS

Employee monitoring: 5 things to consider

Employers should consider the following before implementing any form of employee monitoring:

Is there really a problem? Does the business really require making an investment in employee monitoring? These are practical questions that require an honest assessment before implementing monitoring.

Which laws apply? Understand the laws discussed in the article.

Understand the technology. Beyond ensuring any particular technology is reliable and effective, consider how much the technology intrudes upon employees' privacy.

Notify and educate employees. Implement a policy that clearly sets out the type of monitoring that will be conducted, and states employees will have no expectation of privacy over their use of the company's computer systems.

Anticipate morale issues. Deal upfront with anticipated employee concerns and think about how the company's monitoring practices may discourage some people from applying for work at the company.

er clearly tell all employees they may be monitored. Arguably, an employee who is notified of such a policy implicitly consents to the monitoring, assuming he continues to work.

By understanding technology, legal obligations and employee culture, employers can implement employee monitoring programs in a way that achieves objectives while reducing the risk of legal disputes and poor employee morale.

Adrian Miedema is a partner and Andy Pushalik is an associate with Fraser Milner Casgrain's employment group in Toronto. Adrian can be reached at adrian.miedema@fmc-law.com and Andy can be reached at andy.pushalik@fmc-law.com.