workplace.ca A DIVISION OF: THE INSTITUTE OF PROFESSIONAL MANAGEMENT TUESDAY, NOVEMBER 01, 2011

features

featurearticle

What Every Smart Employer Should Know About Monitoring Employee E-Mail

By Alan Riddell, Steve Shaddock and Gillian Bilton

Employers have a right to know if their employees are abusing company computers and e-mail, but the law imposes some restrictions on how far they can go to spy on their employees' e-mail and internet use. Employees have certain privacy rights and there are limits on how far you can go to monitor your workers without violating those rights.

The conflicting rights of employers and employees over computer use is another Internet age showdown which is already beginning to have a profound impact on companies and the workplace. How do you know whether your employees are working as opposed to web surfing, social networking, shopping, downloading, viewing or sending pornography or racist material, sending degrading messages about colleagues or customers, running an illegal business or stealing confidential company information? The consequences of leaving your employees totally unmonitored can be expensive and sometimes even catastrophic. Take Chevron, which paid $2.2 million in damages for sexual harassment stemming from jokes sent through an employee's e-mail. In a similar case in 1997, a racist joke sent via an employee's e-mail gave rise to a $60-million lawsuit.

In this kind of environment, smart employers have clear policies that recognize their workers' privacy but also set restrictions on computer use which they carefully monitor to ensure compliance by their employees.

Privacy Protection in the Law

The *Personal Information Protection and Electronic Documents Act* ("PIPEDA") is federal legislation that outlines what is reasonable in workplace surveillance. Employers must demonstrate that any intrusion of privacy is limited to what is "absolutely necessary". Other than PIPEDA, there is no specific legislation in Ontario governing the privacy rights of persons employed by provincially-regulated businesses.

Privacy rights are recognized in the Charter of Rights and Freedoms (Section 8), the Criminal Code, and also at Common Law. For example, section 184 of the Criminal Code makes it a criminal offence to "wilfully intercept a private communication" using a device, such as a computer. Although this seems very broad, the Criminal Code defines "private communication" as "communication made under circumstances in which it

is reasonable for the originator to expect that it will not be intercepted by any other person".

Finding the "Reasonable" Balance

Privacy rights are not absolute and must be balanced against employers' legitimate business interests. Employers can monitor e-mail and internet use (including access to e-mails and computer files) so long as such monitoring is done reasonably. The Courts have interpreted this to mean that employers may monitor computers provided that the employees do not have a "reasonable expectation of privacy" in the communication or file. So what does this mean?

A Reasonable Expectation of Privacy?

A reasonable expectation of privacy means that an employee must be able to expect – within reason – that the information they produce or communicate is private or confidential. The Courts have decided that this "reasonable expectation" will depend on the circumstances of each situation, including:

- Whether the employee owned the property or had possession or control of the property/place searched;
- What the property or item was used for;
- The ability to regulate and exclude access (such as using a password);
- The employee's subjective expectation of privacy; and
- The objective reasonableness of that expectation.

The Court shed some light on the issue in a recent decision released in 2011 (R. v. Cole) involving a high school computer teacher who had child pornography on the laptop given to him by the school to use for both work-related and personal use purposes. The school's IT technician found the pornography in a hidden folder on the laptop's hard drive during a routine check-up of the system.

The key issue facing the Court was whether the teacher had a 'reasonable expectation' that the contents of his laptop were private. The Court looked at a number of factors and decided that the teacher did have a reasonable expectation of privacy in his personal use of the laptop for the following reasons:

- The school board gave teachers exclusive possession of the laptops and permission for their use at home, on weekends and during summer vacations;
- The school board gave teachers explicit permission to use the laptops for personal use;
- The teachers used passwords to exclude others from their laptops;
- Nearly all teachers stored personal information on their hard drives; and
- There was no clear and unambiguous policy in place which allowed the employer to monitor, search or police use of the laptops.

But the Court also found the teacher's right to privacy was subject to the "limited right of access by his employer's technicians performing work-related functions" to maintain the system. This means the teacher's privacy rights didn't protect him from the technician finding the pornographic file during routine maintenance. According to the Court, the teacher should have been 'reasonably' aware of the functions the technician had to perform and should have 'expected' this type of access to his computer.

The Bottom Line

This case drives home that employers should have a monitoring policy and should ideally try to obtain consent from employees to monitor their email and computer use. This consent can be a signed agreement or an electronic form that describes the policy and requires employees to click a box indicating their knowledge and consent of the policy.

In summary, the best way for employees to guard against computer and e-mail abuse is through clear policies that spell out the restrictions on personal use of company computers and make clear the data they house is not private and could be subject to monitoring. This makes it difficult for employees to argue they had an expectation of privacy in their computer files.

- Alan Riddell is an Ottawa-based Labour & Employment Lawyer and heads the Soloway Wright Employment Law Group

- Stephen Shaddock is an Ottawa-based Litigation Lawyer who practices Labour and Employment Law

- Gillian Bilton is a Student-at-Law specializing in Labour and Employment Law

- Darrell Mast is an Ottawa-based Lawyer practicing in the areas of Municipal Planning and Expropriation