Employer Surveillance of Employees
Peter Bowal
Law Now; Sep/Oct 2006; 31, 1; CBCA Reference and Current Events
pg. 47

Employment Law

Peter Bowal

Employer Surveillance of Employees

Anyone who is being constantly watched by the boss while working knows the unease of that experience. We don't mind working or explaining what we did, but we don't like being watched while we are working. According to Justice LaForest in the Supreme Court of Canada case of *Duarte* (1990):

> "The very efficacy of electronic [recording] is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."

On the other hand, employers have a legitimate interest in preventing losses and ensuring that the workplace is productive and safe. Technology can effortlessly and inexpensively monitor what we do, say, read, write, and with whom we are interacting. We spend much of our lives at work and some of this may be the employer's business, but most of it will not. What rights of privacy do we have at work?

Employer surveillance must be balanced with employee privacy. The law is spotty in attempting to strike this balance.

The *Charter of Rights and Freedoms* applies to limit government power so it applies to public sector employers. The *Charter* does not explicitly set out any limits on monitoring civil servants, other than that such monitoring cannot take place in a discriminatory fashion on the basis of gender, race, religion, age, etc. Government employers concerned about theft and other loss prevention issues may want to check employee personal domains such as bags, lockers and desks. Or they may want to conduct drug and alcohol testing. These are forms of searches over which there is a reasonable expectation of privacy. They are governed by the section 8 *Charter* right for everyone to be "secure from unreasonable search or seizure."

Under the *Criminal Code*, it is a crime to intercept private telecommunications, including from employees to other employees, a superior, or a union official. Section 184 reads "Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years."

By monitoring email and telephone, employers normally would run a risk of being accused of intercepting the private communications of employees. A major exception, however, is the "one party consent" rule, so that there is no crime where

"a person … has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it." In other words, if either the originator or recipient of the calls wants to record the call surreptitiously, it is legal to do that. If a third party such as the employer, as part of an investigation, wants to record the call, it must obtain either a warrant or the permission of at least one party to the call. Emails are stored on corporate servers and may be outside of this rule. Employers may also receive copies of emails forwarded by others, and this sharing implies consent.

Federal and provincial privacy legislation protects from unauthorized use and disclosure personal employee information held by a government institution (such as civil service employers), regardless of the manner in which it is collected. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) broadly protects electronic information and documents. In the workplace, this information might include keystrokes, websites visited, emails and electronic signatures. It outlines when it is permissible to obtain personal information about an employee, without that person's consent.

Judicial decisions and labour arbitrations have also served to regulate employee surveillance. In *Unisource Canada Inc. v. C.E.P., Local 433* (2004), employees protested the use of nine video cameras. The arbitrator dismissed their complaint, concluding that all nine cameras were required to address theft problems.

Employer surveillance must be balanced with employee privacy. The law is spotty in attempting to strike this balance.

Biometric technologies measure human qualities specifically to identify each individual. They are used to access buildings and computer systems at work. In *Turner v. Telus* (2005), the employee was concerned about the ability of Telus to monitor the times when employees would call in for sick days and verify these with the voice recognition biometric system. The court rejected the complaint, finding that the biometric system was important to maintain the competitive position of the employer and that the information obtained was only for substantial business purposes. The vast majority of employees had consented to the biometric screening.

Safeway introduced hand recognition to control time card fraud. In *Canada Safeway Ltd. vs. U.F.C.W., Local 401*, the union argued this biometric information was a direct invasion of privacy and sought other less invasive methods to reduce time card fraud. Again, in the result, business justification outweighed employee privacy.

In *Zesta Engineering Ltd. v. Cloutier* (2002), the employer accessed the employee's computer. The court ruled that although the employee believed in his right to privacy, the computer at work was the employer's property and the employer could legally access it at any time.

Overall, surveillance of employees has been approved by the courts and arbitrators where the business case can be made for it. The surveillance must be necessary, employers cannot obtain nor use information beyond the business purpose, and the

least invasive surveillance should be used. Information collected but no longer used should be discarded. Ideally, consent from the majority of the workforce should be demonstrable. New technological surveillance is acceptable as long as it conforms to these guidelines.

We behave differently when we know we are speaking in the presence of a microphone and camera. We will not always know today when those devices are trained on us. Employers also sometimes monitor employees' movements and behaviour outside of work, including through private detectives. The days of the beeping recording device, visible cameras in the hallway and delete-able email message are gone. All communications, oral and written, and our movements can leave a footprint in technology today. Real privacy at work is elusive. The next time we call in sick, send an email, speak on the telephone, stay late at work, or put something in our briefcase, we should be aware that the employer might be watching.

All communications, oral and written, and our movements can leave a footprint in technology today. Real privacy at work is elusive.

Peter Bowal is a Professor of Law with the Haskayne School of Business, University of Calgary in Calgary, Alberta.