



FRASER MILNER CASGRAIN LLP

RFID Technology: Taking Employee Monitoring to a Whole New Level

By Curtis McDonnell of Fraser Milner Casgrain LLP's Toronto office © CCH Canadian Limited.

Employers who want to monitor their employees more closely or increase their control of restricted areas in their places of business have a new tool at their disposal—Radio Frequency Identification Devices (“RFIDs”). This technology provides enhanced security and is less intrusive and less expensive than more traditional methods such as finger or thumbprints, palm prints, or retinal scans. Other reasons for the attraction to RFIDs are their small and inconspicuous size and the amount of information that can be stored in the tiny memory chip.

RFIDs fall into two major categories: active and passive. Active RFIDs require their own power source in order to transmit the information contained in their memory to a receiver. Passive RFIDs have no power source of their own. They are activated by a scanner or reader that has an external power source and can read the information contained in the memory of the RFID. In some ways, an RFID is like a bar code which gets scanned at the supermarket when checking out purchases. The big advantage of RFIDs is that they do not have to be in close proximity to the scanner. The information on the memory chip can be scanned and read remotely at distances from a few inches to several feet away.

Currently, RFIDs are used to track shipments of goods from manufacturers to retailers. This enables both the manufacturer and the retailer to control the inventory flow and supports a “just in time” supply chain. They are also used to verify the authenticity of expensive products such as purses and briefcases when these items are returned for repair or refund. With a bar code scanner, we are usually aware that an item is being scanned. However, from a privacy perspective, one of the problems with RFIDs is that the scanning can take place without the individual knowing about it.

This can lead to privacy law issues. For example, where an individual uses a credit card to buy a product with an RFID embedded in it, there is the possibility of matching the RFID information with the personal information obtained from the credit card. As a result, the person buying the goods, purse, sweater, shirt or suit theoretically could be tracked through the RFID after leaving the store.

RFIDs have now been developed that can be implanted in humans and scanned remotely. The U.S. Food and Drug Administration has licenced one organization, VeriChip Corp., to manufacture and sell these chips for implantation in humans. The chip is about the size of a grain of rice and is implanted beneath the skin.

These subcutaneous chips are currently being used in a number of applications, including the identification and monitoring of patients with Alzheimer’s disease. Some chips have been implanted into patrons of a Spanish nightclub, which allows these VIP clients to jump the queue avoid lineups to the club.

There has been significant reaction by a number of states to the threat to the privacy rights of individuals presented by this technology. In fact, Wisconsin, North Dakota, and California all have passed legislation that prohibits employers from inserting RFIDs in employees without the consent of the employees. The legislation in California creates a civil right of action whereby a person “chipped” against his or her will can sue and recover up to \$10,000.

We already have seen in Canada, employers using finger and thumb prints, voice recognition software, and even GPS(global positioning systems) to monitor employees and manage the workplace. Generally, employers have been able to make out a case that the technology and its use in the workplace is reasonable and that the personal information is properly safeguarded, its use limited. However, none of these technologies involves implanting a device in the employee.

Another concern about these types of RFIDs is that, at the moment, the information on them is not encoded. This means that anyone with a scanner can read what is on the chip. Although this can be dealt with by encrypting the information on the chip, this must be built into any program that places employee information on a chip prior to implantation in the employee.

In Canada there is no RFID legislation comparable to that in some parts of the United States. However, since the technology exists, there should be no doubt that some employers, especially if they are involved in highly sensitive and secretive work, may be tempted to introduce such a technology in order to increase their ability to monitor not only their premises but who is accessing the sensitive areas of the workplace. The question, then, is whether it would be a reasonable demand by an employer that carries on a business where access has to be strictly limited to authorized employees, to require an employee to consent to the implant of an RFID as a term of employment?

Canadian privacy legislation requires a balancing of the employer’s right to collect, use, and disclose appropriate personal information to manage the employment relationship against employees’ right to privacy. The collection, use, and disclosure of personal information has to meet the reasonable person test. Will subcutaneous RFIDs ever meet this test? Given how invasive this technology seems to be it is difficult to imagine, for the immediate future, how any employer that wants to use this technology in its workplace, will be able to satisfy the reasonable person test which the Canadian law requires.