

A Brave New World: Biometrics in the Workplace

November 6, 2008

Cappone D'Angelo
Tina Giesbrecht

Everyone is familiar with the use of fingerprints in the criminal context. But are you also aware that employers are increasingly using employees' biological characteristics, such as a person's finger, hand, voice or facial features, to identify and keep track of employees' attendance and work hours? The use of biometric technology in the workplace gives rise to a number of privacy issues. Two recent Investigation Reports from the Alberta Information and Privacy Commissioner provide guidance on these issues in this brave new world.

Empire Ballroom

The Empire Ballroom nightclub in Edmonton sought to introduce a thumbprint sign-in system to monitor employee attendance and calculate payroll. A former employee complained to the Commissioner that, among other things, the thumbprint system was introduced contrary to the Alberta Personal Information Protection Act (PIPA).

The Ballroom had previously used a punch-clock system for attendance and payroll. However, the punch-clock allowed employees to access each others' timecards and punch in other employees who were absent or late ("buddy punching"). To address this problem, the Ballroom required managers to initial employees' timecards when they came in and left work. This turned out to be an onerous, inefficient process. As a result, the thumbprint sign-in system became an attractive alternative.

Unlike older biometric identification systems such as police fingerprints, new biometric technology does not actually store copies of employees' thumbprints and identify them one-to-one with the copy. Instead, the thumbprint sign-in system used by the Ballroom first measures the unique attributes of an employee's thumbprint, then using an algorithm, turns those attributes into a unique number that is stored and encrypted in the database. The number cannot be reverse-engineered to create an image or obtain the measurements of the employee's actual thumbprint.

The Ballroom asked all employees to scan their thumbprints into the new sign-in system. Employees were told that their thumbprints were going to be used as a sign-in/sign-out procedure, but were not informed how the technology worked or what information it collected. The complainant refused to scan her thumbprint because she felt that her fingerprints were highly sensitive information and the use of such information for attendance and payroll was intrusive and unnecessary.

The Commissioner confirmed that an employee's biological characteristics and the unique number stored in the system are the employee's personal information. In this case, the Commissioner also found that the information was "personal employee information."

"Personal employee information" under PIPA is information reasonably required by an organization that is collected, used or disclosed solely for the purposes of establishing, managing or terminating the employment relationship. Employers may collect, use and disclose such information without consent, but must notify employees about the collection, use or disclosure and the purposes of it.

The Commissioner confirmed that attendance and payroll are reasonable aspects of managing employees. The Commissioner also found that the additional personal information collected by the thumbprint sign-in system was reasonable for attendance and payroll purposes because the Ballroom's previous systems did not work. A key to the Commissioner's decision was that the Ballroom was not actually collecting

employees' thumbprints but simply the unique identifying number.

However, the Commissioner also found that while employees were notified of the purposes of collecting the thumbprint information, they were not adequately informed about what personal information was in fact being collected and used. As a result, the complainant and other employees believed that their actual thumbprints were being collected and used, as opposed to just the unique identifying number. The Commissioner stated that, under PIPA, employers must inform employees about the specific information to be collected, used and disclosed for specific purposes, so that employees can make meaningful decisions about their personal information. Because the Ballroom's employees were not adequately notified about the specific information being collected, the Commissioner found that the Ballroom had breached PIPA.

Southwood Care Centre

A very similar approach was taken by the Commissioner in a case involving Southwood Care Centre, located in Calgary. In that case, an employee complained about the employer's plans to introduce a hand scanner for employees to use when clocking in and out of work. As in the Empire Ballroom case, the Commissioner found the introduction of this technology to be acceptable in part because:

- the hand scanner did not actually record finger prints or palm prints – instead, an algorithm converted these images into one mathematical value, which was then stored in the system; and
- the employer had sufficient evidence to establish that alternative authentication systems would not meet its business needs. For example, there was evidence of a problem with "buddy punching" and evidence of an administrative burden when employees forget, lose or damage swipe cards.

However, as in Empire Ballroom, the Commissioner found that the employer's notice to the employees of the collection of the information was not sufficient. The Commissioner stated the best approach would have been to:

- provide proper notice at the time employees were initially registered in the hand recognition system; and/or
- provide proper notice on a poster near the hand scanner that would be seen each time employees clocked in and out.

Proper notice includes informing the employees of (i) the purpose for which the information is collected; (ii) the specific legal authority for the collection; and (iii) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

McCarthy Tétrault Notes:

These two Investigation Reports from the Information and Privacy Commissioner of Alberta will help employers understand their privacy obligations related to using biometric technology in the workplace.

Here are some tips:

1. Use newer biometric technology that does not actually collect or store employees' physical information, as it is more likely to pass privacy muster.
2. Give proper notice of the collection to the employees, as described above. Explain to employees exactly what personal information is being collected, used and disclosed by the technology, as well as the purposes for doing so. In addition to being required by PIPA, employees who do not understand the limitations and safeguards of the technology are more likely to feel like their privacy is being invaded and may refuse to co-operate.
3. Be prepared to justify the introduction of biometric technology by pointing to deficiencies experienced with other time-keeping or attendance systems, such as "buddy punching" or lost data.
4. Do not immediately discipline an employee who refuses to co-operate with the introduction of new technology without investigating his or her concerns. Employees may have religious objections to such technology that must be accommodated. Alternatively, employees may have a reasonable belief that the technology infringes PIPA. It is important to remember that PIPA prohibits adverse action against an employee who refuses to do something he or she reasonably and in good faith believes is contrary to PIPA.

Employment

[read /](#)

Labour

[read /](#)

Privacy

[read /](#)