

Biometrics in the Workplace - Where to Draw the Line?



"Oh, can't complain."

**Personal Information Protection Act Conference 2006,
April 26 and 27, 2006, Calgary, Alberta**

Gary T. Clarke

Fraser Milner Casgrain LLP
1500-1040 West Georgia Street
Vancouver, British Columbia
V6E 3P9

Direct Line: 604-443-7133
Facsimile: 604-683-5214
E-Mail: gary.clarke@fmc-law.com

I. Introduction

Biometric identification uses specially developed technology to identify an individual on the basis of a unique personal characteristic such as their hand and finger geometry, signature verification, keystroke dynamics, facial recognition, voice recognition, retina or fingerprint. In 1999, Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario reported in her paper entitled “Consumer Biometric Applications: A Discussion Paper”¹, additional biometric technologies under development or presently being used by law enforcement and the military. These included vein patterns (looks at the unique pattern of blood vessels that form when a fist is made), ear shape (of outer-ear, lobes and bone structure) and body odour (at p. 12, 13). A biometric is formally defined as a “unique, measurable characteristic or trait of a human being for automatically recognizing or verifying identity”².

This method of identification has been around for quite some time but the sophistication of the technology has been rapidly increasing and the costs of implementing it has been steadily decreasing. This increased sophistication and decreased cost, coupled with the security concerns that have become front-and-centre since the events of September 11, 2001 and the apparent need/desire of business to go faster more efficiently, has resulted in a significant increase in the use of biometric devices in the workplace. This trend will undoubtedly continue.

The greatest feature of biometric identification is that it is usually very accurate and cannot be easily faked. For example, an airline that uses retina scans to verify the identity of crew members prior to flights ensures everyone is who they say they are, thereby promoting safety and security. A manufacturer might use a hand scan to prevent “buddy punching”, ensure an accurate payroll, manage overtime and time worked under averaging agreements or variances, manage absenteeism or to know with precision who is where in the workplace in the event of an emergency.

“Buddy punching” occurs when one employee punches in for a late or absent colleague or for another that leaves early. It is estimated that employers that use a traditional punch clock would save as much as 2% of annual payroll by eliminating buddy punching by using a biometric system and that such savings would further increase as a result of effectively managing overtime. These systems can automatically alert employers when employees are

¹ This paper can be found at www.ipc.on.ca

² Gary Roethenbaugh, “Biometrics Explained”, www.icsa.net/services/consortia/cbdc/sec.1.shtml.

getting close to overtime eligibility and assist with discipline for absenteeism or lateness by providing a complete and accurate picture of an employee's attendance and punctuality. The benefit to the employee is that their pay-cheque is accurate and overtime is paid in a timely fashion and without question. Employers also report smooth shift changes and a more punctual workforce overall. Aside from the privacy concerns, opponents argue that biometric devices demonstrate a lack of trust and respect and hurt morale, impact on employee individuality, autonomy and dignity.³

So what about the employee's right to privacy? Many employees are already at work 24/7 through the intrusion of email, voicemail and the ubiquitous Blackberry™. Many are also subject to video surveillance, keystroke monitoring, email, telephone and computer-use monitoring while they are at work. Some are subject to alcohol and drug testing. Others are subject to technology that tracks their whereabouts through GPS.

This paper will take a look at how the employee's right to privacy has been balanced (or attempted to be balanced) with the employer's need/desire for improved security and productivity and its other business interests in the context of biometric devices. Other forms of employee monitoring are beyond the scope of this paper but have been addressed by others at this conference. This paper will also provide employers with suggestions and a starting point for evaluating an existing biometric system or for introducing a new one into the workplace.

II. The Legislative Framework

The British Columbia and Alberta *Personal Information Protection Acts* contain provisions that address "employee personal information" (British Columbia) and "personal employee information" (Alberta). In British Columbia, while notice is required to be given to an employee before such information is collected, used or disclosed, consent is not required if the information is reasonable for the purposes of establishing, managing or terminating an employment relationship⁴. Similarly, in Alberta, "personal employee information" is defined as personal information reasonably required by an organization and is collected, used or disclosed solely for the purposes of establishing, managing, terminating an employment or volunteer work relationship (but does not include personal information unrelated to that relationship)⁵. Such

³ IOMA Payroll Manager's Report, May 2004.

⁴ See s. 1, 13, 16 and 19 of the B.C. *PIPA*.

⁵ See s.1(j) of the Alberta *PIPA*.

information may be collected, used or disclosed without consent if the person is an employee and for recruitment purposes. The collection must be reasonable and consist of information that is related only to the prospective employment or volunteer work relationship. In the case of existing employees, reasonable notification must be given to the employee that the information is going to be collected, used or disclosed as well as the purpose for which it is going to be collected, used or disclosed⁶.

These provisions provide important exemptions to consent that would otherwise be required (subject of course to any other available statutory exemptions⁷) and will have an important effect, in my view, on future disputes that arise in the workplace concerning biometrics. To date, I am unaware of any decision made under the British Columbia or Alberta *PIPA* on the use of biometrics in the workplace. To successfully invoke these exceptions, an employer would have to show that:

1. the personal information being collected, used or disclosed falls within the definition of “employee personal information” or “personal employee information” (personal information about an individual collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the employee and the employer (or volunteer work relationship in Alberta)).
2. advance notification of collection, use or disclosure was given to the employee. This notification must be “reasonable” under the Alberta *PIPA*.

The federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* does not have provisions akin to those found in the British Columbia and Alberta *PIPAs* and does not apply in any event to private-sector employees not working for a federal work or undertaking (airlines, banking, telecommunications, etc.).

Finally, it should be noted that although the right to privacy is not specifically referenced in the Canadian *Charter of Rights and Freedoms*, it is considered to fall within s.7 of the Charter which guarantees the right to liberty and security of the person. This right has also been recognized by the Supreme Court of Canada in decisions such as *R. v. Dyment*⁸.

⁶ See s. 15, 18 and 21 of the Alberta *PIPA*.

⁷ Found in s. 3, 12, 15 and 18 of the B.C. *PIPA* and s. 4, 14, 17, and 20 of the Alberta *PIPA*.

⁸ (1988), 55 D.L.R. (4th) 503 at 513.

III. In Search of Balance – A Look at Decided Cases

The following is a discussion of many of the decisions that have been made to date on the use of biometric devices in Canada. While the facts of each case differ, there are some important similarities and as a result, we are able to distill a list of considerations and factors that any employer considering introducing a biometric system in their workplace (or preparing to defend an established one) should bear in mind. The discussed cases are organized by technology – hand scanning, voice prints and partial finger scan.

Hand Scanning

In *Cascadia Terminal and G.W.U., Loc. 333 (Re)*⁹, Arbitrator Ready dealt with a dispute that involved the implementation of a time keeping system that measured employee hands as they clocked in and clocked out.

Initially, the employer had a traditional time clock system. This was replaced in 1991 with a manual timesheet system. The stated reason for the change was to “place more emphasis upon the honesty and integrity of [the] employees, and generally place the responsibility of time recording where it belong[ed], with the individual employees” and that such a change would assist the goal of “humanizing the working environment” and “better the overall morale” of employees. These stated reasons would prove to be a thorn in the employer’s side for the next 13 years.

In 1996, the employer wanted to implement an electronic time keeping system. The union opposed it.

In 1997, the employer wanted to implement a direct deposit banking system for employee pay cheques. While this is now commonplace, it was seen as a significant change by the union at the time. The union’s view was that if it agreed to this direct deposit system, the employer would back away from implementing an electronic time keeping system. The parties met and the employer issued a memo to all employees that stated that the timesheet system

⁹ (2004) 123 L.A.C. (4th) 203

would continue and that there would be “no punch/swipe clock instituted now *or in the future* as a result of the new system”. The employer would regret these words for the next 7 years.

In 1998, the employer advised the union that it intended to implement a phone time keeping system. The union grieved, arguing that the employer’s memo was a commitment to never institute an electronic time keeping system. The arbitrator held that this memo was not a legally binding agreement and did not commit the employer to never implementing an electronic time keeping system. However, the employer was estopped from doing so during the term of their collective agreement to allow the union the opportunity to bargain on this issue. The employer was thus, hamstrung until December 31, 2000 when the collective agreement expired.

After its expiry, the employer advised the union that it was going to implement a form of punch clock time keeping system. The union protested, arguing that they had not yet been given the opportunity to bargain this issue. Four months later, the employer again advised the union that it was planning to implement a better timekeeping system. Again, the union protested by stating that the employer could not do anything in this regard until negotiations had concluded. The employer disagreed.

Collective agreement negotiations ultimately broke down and a lockout occurred in 2002. This resulted in an interest arbitration that established a renewed collective agreement between the parties. There were a number of outstanding issues, however, and the parties were urged to resolve them on their own, failing which they would be resolved by arbitration. The proposed hand recognition timekeeping system was one such issue.

At the resulting arbitration, the employer argued that it had the right to implement the system under its management rights and that it did not need the union’s agreement to do so. It argued that the manual timesheet system was cumbersome and inaccurate. In contrast, the new system recorded an individual’s hand size and shape and then subsequently recognized these dimensions when the employee clocks in and out. This would ensure accurate time recording and allow the employer to determine with precision who was in the plant at any given time for safety reasons. This new system was also expected to reduce the costs associated with processing payroll.

The union argued that the proposed hand recognition system violated the employees' privacy rights. It stated that the employees should have the right, not the employer, "to voluntarily control what information about themselves they will give to others".

The union also argued that the system was also inappropriate because of health and safety concerns (dryness to the hands and transmission of diseases by using the scanning device). Finally, the union argued that such a system would cause stress amongst the employees and would undermine the reasons why the traditional time clock system was eliminated in 1991 (increased trust and morale).

Arbitrator Ready concluded that the employer had the right to change the timekeeping system and implement a new one and that the collective agreement did not fetter this right. In reaching this conclusion he considered the following four factors:

1. The purpose of the practice;
2. The impact of removing or continuing the practice;
3. The day-to-day efficiency of the operation; and
4. The impact on employees.

The purpose was identified as the need to accurately record time so that employees are properly paid.

The impact of continuing the manual timesheet system was identified as continuing inaccuracies (this also addressed the day-to-day efficiency of the operation).

The impact of removing the manual timesheet system (and the impact on employees) was stated by the union to be "dehumanizing the workplace and making the employees feel like they are not trusted" and that the hand recognition system "could be characterized as an invasion of privacy because of its data collection and the potential uses of such data". Arbitrator Ready found that the union had not substantiated its privacy concerns:

Many of its concerns related to the very issue upon which the Employer moved away from the time clock in 1991. But a lot has happened since 1991. When technology was first being introduced into the workplace and into our personal lives, individual's privacy appeared to constantly be invaded -- whether that

took the form of the computer on one's desk(s), the deposit of one's cheques directly into one's bank account, the withdrawal of one's funds via an encoded card such as a debit card, etc. Society was constantly being bombarded with such concerns and the workplace was no exception. However, times have changed. Now, on average, every home has at least one computer with Internet links around the world and our personal data being exchanged on international circuits. Individuals now use their debit cards in any country while traveling, and if they lose the card they feel very inconvenienced. By making these statements, I am not invalidating the Union's concerns. I think they are valid and it is incumbent upon the Union to bring them to the Employer's attention. However, the Employer has been faced with varying concerns since 1998 when the Union first raised the grievance. It is now six years later and time to move forward.

He also found that the union had not substantiated the health concerns.

In the result, he concluded that the employer could move to a new timekeeping system "whatever that system might be, subject only to the raising of valid concerns and the employer being willing to listen to those concerns".

In another hand scanning case, *Canada Safeway Ltd. and United Food and Commercial Workers Union, Local 401*, Arbitrator Ponak concluded that the hand scanning devices the employer had introduced into the workplace were permissible and dismissed the three grievances that had been filed that challenged the devices as an unjustified invasion of privacy. Like the system in *Cascadia*, the devices were to be used for payroll and attendance purposes. The Arbitrator agreed with the union that employee privacy was infringed, but agreed with the employer that this infringement must be balanced, proportionately, with the employer's business needs and interests. This proportional balancing approach was adopted from *PIPEDA Case Summary #281* (discussed below) and framed as "the more intrusive the impact on employee privacy the greater the business rationale that must be demonstrated. Conversely, if the intrusion on employee privacy is insubstantial, the concomitant level of justification also is lower".

Arbitrator Ponak found the intrusion to be "relatively low" because:

1. The method of collection was not "physically intrusive, time consuming, painful or harmful".
2. The collected information was kept as a numerical template that revealed nothing. It had no other use and was a one-to-one matching system.

3. The template could not be reverse engineered and as such the template revealed “far less about the individual’s personal characteristics than other commonly retained employee information such as photographs or physical measurements such as height or weight”.
4. The template was not necessarily unique because the same template could be shared by 1% of the population.
5. The template and system were very secure.

As a result of the finding that the intrusion was low, the employer only had to meet a test of reasonableness “rather than some higher standard, such as safety necessity or company survival, as might be required if the intrusion into employee privacy was greater”. This was not difficult to do. The employer had evidence of buddy punching and other forms of time card deception. It also had evidence of errors caused by the traditional time card punching system and evidence to support its position that the new system would be more efficient and would eliminate errors. The Arbitrator rejected the union’s suggestion that alternative, less intrusive options existed such as installing video cameras at the punch clocks or installing a swipe card system. These suggestions were seen as creating their own problems while not solving the problems posed by the punch clock system.

Of interest, the Arbitrator also ordered the employer to develop written policies on how employees were to be removed from the system upon termination and provided appropriate training on the use of the system. He also ordered that the nature of the technology be clearly conveyed to the employees because it was apparent that much mis-information about the system had been spread (for example, many incorrectly believed that the system recorded finger and palm prints).

Voice Prints

In *PIPEDA Case Summary #281*, the Assistant Privacy Commissioner of Canada considered a complaint from a group of employees that their employer was requiring them to consent to the collection of biometric information (a voice print) to enable them to access their employer’s business applications (i.e. to log work-related information and report absences). This use of a voice password system was introduced to allow employees, particularly those in the field, to log work information in a “secure, efficient and cost-effective manner”. About 20% of

the workforce was required to use this system. The enrollment process was described by the Assistant Commissioner as follows:

To register, the employee places a phone call during which he or she will have spoken a series of digits several times. The system software converts the spoken digits into a matrix of numbers that represent the behavioural and physical characteristics of the way the individual speaks and his or her vocal tract. The voice print is used solely for authenticating the employee when he or she is accessing the business applications. It does not play a role in any of the applications.

The system was introduced largely for security reasons (a voice print is more difficult to crack than a password). The employer was noted to manage large amounts of customer data and protection from unauthorized access was critical. As an added bonus, the system was less costly than password systems and the ability to access the business applications by telephone streamlined their business by eliminating paper-based processes.

The voice prints were stored in a secure database. Access was highly restricted and limited. Those that had access could not “change, interpret or substitute the record, and the voice print cannot be reverse-engineered to synthesize a voice. Therefore, there is no possibility of any fraudulent misuse of someone’s voice.” The system compared the voice print to the employee’s own stored voice print (one-to-one match as opposed to one-to-many authentication) and could not be used for any other purpose.

The Assistant Commissioner dismissed the complaint and deemed employee consent to the use of the system. It was noted that the purpose of *PIPEDA* was to balance the individual’s right to privacy with the organization’s need to collect, use or disclose personal information for appropriate purposes. This balancing exercise was characterized as one of proportionality (i.e. was the loss of privacy proportionate to the benefits the employer would gain). Here, it was concluded that the balance favoured the employer and that the benefits of the system outweighed what was described as a “fairly benign” infringement of the employees’ privacy.

This conclusion was also driven by the finding that the voice print did not reveal much information about the individual, there was no possibility of improper use, that it was one-to-one authentication system and that a breach of the customer’s privacy (as a result of not having this system in place) would seriously damage customer confidence - possibly resulting in “enormous” losses to the employer.

The Assistant Commissioner did, however, make it clear that not just any privacy infringing measures or systems would be appropriate and that the individual circumstances must be considered and balanced. The employer was also ordered to remove an aspect of the system that prompted employees to report the reason for an absence as this was seen to be excessive.

In *Turner v. Telus Communications Inc.*¹⁰, the Federal Court of Canada dealt with a complaint that had been filed by a group of its employees that were concerned about technology that Telus introduced in 2002 called “e.Speak”. Although the decisions of the Privacy Commissioner of Canada are issued on an anonymous basis, *Turner* is the obvious sequel to *PIPEDA Case Summary #28*. Displeased with the result, the employees decided to seek relief from the Court. Such a step is not by way of a judicial review but as a fresh application - truly “another kick at the can”.

Turner provides more detailed information about the biometric system, including the fact that once accessed, the voice of the employee is stored for a period of 1 to 2 months. It is also noteworthy that Telus had advised the employees that if they did not enroll in the system (by submitting their voice print), they would be subjected to unspecified progressive discipline.

The employees sought an declaration that Telus had breached *PIPEDA*, an order that it cease and desist from doing so, an order that it publish a notice of the action taken to correct its practices, an order for damages for humiliation caused to the employees, and costs.

The applications were dismissed. Mr. Justice Gibson found:

1. that the voice print was “towards the lower end” of the spectrum of privacy intrusion.
2. that a factor in determining whether an expectation of privacy was reasonable was whether or not the information was already available to others and noted that a person’s voice was communicated on a daily basis to others.

¹⁰ [2005] F.C.J. No. 1981

3. that regard must be had to the present circumstances, not to what the circumstances might in the future become: “I am satisfied that the test of what a reasonable person would consider to be appropriate in the circumstances must be applied against the circumstances as they exist. I accept that circumstances can change, that new uses and applications can be contemplated and adopted, and that new technologies to breach security can be developed. I am satisfied that new uses and applications, and changes in technology that might render Telus’ security precautions inadequate, are to be tested only when they are real and meaningful, not when they are hypothetical”.
4. that Telus had *bona fide* business interests/objectives in implementing the system and these were met by the biometric system.
5. that proportional balancing favoured the biometric system over the limited privacy intrusion and that a reasonable person would see the collection of the voice print to be reasonable in the circumstances.
6. that the security measures and safeguards taken were appropriate.

Against the background of these findings, Justice Gibson had to address the issue of whether Telus had met its consent obligations under *PIPEDA*. He concluded that it had and utilized ss.7(1)(a) of *PIPEDA* which provides an exception to consent where collection is clearly in the interests of the individual and consent cannot be obtained in a timely way. The Court did not, however, address how the collection would clearly be in the interests of the non-consenting employees. This approach effectively confined the impact of the Court’s decision to the applicant employees and would not “enable Telus to proceed with full and complete implementation of e.Speak and to force employee enrollment” but would “enable Telus to continue with the implementation of e.Speak at its current level” and if others refused to consent, Telus could proceed with progressive discipline. Obviously concerned with the nature of this solution, the Court also offered an alternative - a finding that Telus had fulfilled its consent obligations under *PIPEDA* in relation to the system’s implementation and that those who refused to consent going forward would undoubtedly be subjected to progressive discipline and the impact of this would be “for another day and for another forum”.

In other words, Telus got the green light to continue with its implementation, the applicant employees’ consent was disposed of under ss.7(1)(a) and a signal was sent to all other employees that a refusal to consent would likely be met by progressive discipline. Arbitrators

hearing grievances filed as result of such discipline would certainly have been provided with copies of the decisions of the Privacy Commissioner of Canada and the Federal Court by Telus to support Telus' position.

It should also be noted that the Court did express some displeasure with the Telus' "high handed" conduct through the enrollment process and its failure to consult with the union about the implementation of the system.

Partial Finger Scan

In *IKO Industries Ltd. and U.S.W.A., Loc. 8580 (Re)*¹¹, Arbitrator Tims had the opportunity to consider whether the employer had the right to replace its swipe card timekeeping system with a biometric payroll and timekeeping system in one of its shingle manufacturing plants. The union's position was that the proposed system was an unwarranted invasion of privacy, inconsistent with the employer's management rights. The employer's position was that it was necessary, did not amount to an invasion of privacy, and was within its management rights.

The new system involved scanning the index finger of employees as they clocked in and out. When enrolling in the system for the first time, the system scanned the ridges under the skin of a non-continuous portion of the employee's index finger in order to create a mathematical template that enabled it to recognize the employee on subsequent occasions. It did not make or store a copy of the employee's fingerprint nor did it attempt to match the scan with a database of other employee scans. Only six employees of the technology supplier had the ability to replicate the image using the mathematical template and even if they did so, it would not be of any extraneous use.

The employer had implemented the new system (or was in the process of doing so) at its nine other Canadian plants. One other grievance had been filed alleging a breach of *PIPEDA* but that it had been withdrawn on a without prejudice basis.

Although the employer had not commissioned a study to determine how much more efficient the biometric system would be than the swipe card system, it estimated that the

¹¹ (2005) 140 L.A.C. (4th) 393

new system would save supervisors 10 minutes of time per employee per pay period and that the payroll clerk's workload reduction would also be significant. The employer also argued that the new system would be more accurate as a result of the elimination of manual steps and would ensure that the employee clocking in and out is who s/he says s/he is. The prevention of "buddy punching" was alluded to by the employer, but there was no evidence that this had been a problem. The employer also argued that the new system enhanced security and safety by allowing the employer to know, with exact certainty, who was in the plant (and specifically where in the plant) in the event of an emergency.

It should be noted that the employer engaged in significant consultation with the union and its members regarding the introduction of the biometric system. Detailed information was provided and posted on the bulletin board and presentations were given. However, when the employer began the enrollment process, only three employees participated and the union filed its grievance. After its filing, the employer offered to send all of the members of the union executive (at the employer's cost and with full pay) to the technology supplier's offices in Montréal to allow them the opportunity to fully understand the technology and have their concerns satisfied. The union initially refused this offer, but eventually relented and the meeting in Montréal took place. It did not, however, resolve the matter and the grievance was arbitrated.

The union's membership had voiced concerns that the technology would be used for purposes other than timekeeping and that they feared that they would have no control over the use of their personal information, which they feared would be used to do background checks, credit checks, and generally "to keep track of them" and to "do constant surveillance of them".

At the hearing, the union argued that:

1. absent clear language in the collective agreement, the employer had to justify the invasion of privacy (the management rights clause was said to be insufficient).
2. workplace privacy rights were recognized and accepted by arbitrators and the technology at issue invaded those rights because it collected information about the employee's physical features without their consent.
3. it was skeptical that sophisticated hackers could not reverse engineer the finger scan.

4. while the finger scan, if reverse engineered, might presently be useless, it could become useful in the future as technology evolved.
5. the burden was on the employer to justify the introduction of the system and that it had failed to do so, noting that the employer had not conducted a study on the efficiency of the present system or on the alternate swipe card system offered by the same supplier.
6. there were less intrusive means available to address the stated need for a more efficient and accurate payroll system (including the swipe card system).
7. the only objective not addressed by the swipe card system was identity verification and that this was akin to permanent surveillance and could not be justified given that there was no evidence of abuse tendered by the employer. This failure, together with the extensive security already in place (guardhouse, cameras), the availability of alternatives and the fact that the business (shingle manufacturing) was not of a sensitive, high risk nature made the intrusion unseemly and unwarranted.

The employer argued that:

1. the burden was on the union to show that the biometric system was an invasion of privacy.
2. the employer had the right to introduce the new technology under the terms of the collective agreement and that such a right could only be abrogated if the union could show individual hardship or injustice.
3. the collective agreement contained other clauses that were more invasive to employee privacy than the proposed system (i.e. the provision of names, address, and telephone numbers to the union every six months).
4. the technology proposed did not invade privacy, did not amount to surveillance and proper safeguards were in place.
5. the data that would be maintained by the new system was the same as the data already in its possession and that the only difference was the requirement that the employee place their index finger on a scanner for 2 seconds.

6. the system was only intended for timekeeping purposes and to control site access, and not to prevent “buddy punching”.

Arbitrator Tims agreed with both parties that subject to express collective agreement terms, employees enjoy workplace privacy rights but that these rights must be balanced with the competing interests and rights of their employers to make rules to further their business objectives. She also agreed with the employer that the union carried the burden of showing that the system was invasive of employee privacy.

On the strength of other authorities, Arbitrator Tims noted that there is a spectrum of privacy interests and that some invasions will be much more intrusive than others. On this spectrum, the biometric system at issue was seen to be on the lower end (not an “egregious disregard of privacy rights”), but an invasion of privacy nonetheless. Her attention then shifted to the available safeguards. Citing discussion papers written by Dr. Ann Cavoukian, she noted that while the system incorporated a number of security safeguards, there were some important deficiencies in the system or in the evidence before her. For example:

1. there was no evidence about what would happen to the mathematical template after an employee’s termination.
2. the mathematical template would be in the employer’s possession and not in the possession of the individual employee to whom the template relates.
3. the template could be accessed by at least six representatives of the system supplier and reverse engineered.

She also noted her agreement with the union submission that just because the information, even if recreated, would not be useful did not justify the invasion of privacy.

Finding an invasion of privacy, Arbitrator Tims proceeded to balance this invasion with the business interests of the employer. The scales were balanced as follows:

1. Improved Efficiency of Payroll - She agreed that the biometric system would meet this legitimate business objective but that the alternate swipe card system offered by the same supplier would also meet this objective but without the invasion of privacy.

2. Increased Security and Controlled Site Access - She agreed that the biometric system would enable the employer to know precisely who had accessed the premises and that there was no assurance that the person who swiped the card was the person to whom the card belonged. However, this was characterized by the Arbitrator as a want rather than a need. There was evidence that the plant had a guardhouse (staffed around the clock), a single entrance and security cameras. There was limited evidence of security concerns, only anecdotal evidence of historical “buddy punching”, evidence that a failure by an employee to show up to work would be noticeable and evidence that the business was not high risk or security sensitive.
3. Emergency Response - She agreed that the biometric system would enable the employer to know, with certainty, who was in the plant (and where) in the event of an emergency. However, she noted that there was no evidence of emergency situations in the past that required evacuation and noted the evidence that the employer could get a good idea of who was on the premises by looking at the existing swipe card system.

In the result, the Arbitrator ordered that the employer cease and desist from introducing the biometric system. In so doing, she noted that her decision arose from the individual facts of the case and was not to be seen as a “general proscription” against biometrics.

IV. Lessons Learned

The previous decisions provide employers with some helpful guidance when deciding whether or not to implement a biometric system in their workplace, discontinue such a system, or revise or improve an existing system to insulate it from successful challenge.

The following lessons or suggestions are offered:

1. Have a good (and defensible) reason for wanting to implement the biometric system. Be sure that the proposed system does what you want it to do and that the benefits are known. In *IKO Industries*, the employer had not done its due diligence to determine what it would save in terms of payroll efficiency by introducing the biometric system. Also, as noted in *PIPEDA Case Summary #281* and *Canada Safeway*, the more intrusive the impact on employee privacy, the greater the business rationale that must be demonstrated.

2. Consider the message a biometric system may convey and its impact on the business. Will it communicate to employees that they are not trusted and adversely impact morale? In *Cascadia*, the employer initially switched to a manual timesheet system to place more emphasis on trust and integrity, humanize the workplace and improve morale but then moved to a biometric system a few years later. Mary O' Donoghue notes that studies have shown that where there is an excessive degree of monitoring, there is a correspondingly high degree of employee stress and that this can be more expensive for employers in terms of stress leaves and loss of valued employees¹².
3. Consider whether there is an alternate way to achieve the same end. The failure to consider less intrusive alternatives was a major factor in cases such as *IKO Industries* (where a swipe card system from the same supplier was available that would meet the employer's stated objective of payroll efficiency). It may also be possible to provide an alternative to the biometric system for employees that are uncomfortable with providing biometric information.
4. To the extent possible, collect as little biometric information as possible in the least intrusive way possible. In *IKO Industries*, the technology looked at only a portion of the ridges below the skin of the index finger and the mathematical template that was created had gaps, as opposed to taking a complete fingerprint.
5. Ensure that biometric information is collected in an open manner. If possible, consult with the union and affected employees well in advance of the proposed implementation date¹³. If buy-in can be accomplished and consent obtained (even if consent may not strictly be needed under *PIPA*), the implementation process will naturally be much easier. As can be seen from cases such as *Canada Safeway*, misinformation about biometric systems can spread among employees that can make it much harder to implement the biometric system.
6. Ensure strict security and safeguards are in place. The less vulnerable the biometric system, the better it will fare before an adjudicator. A biometric system that: (a) has limited memory; (b) has limited access; (c) encrypts and destroys the original data after the encryption occurs; (d) maintains only a mathematical template and makes it impossible to reverse engineer or reconstruct the biometric

¹² Mary O'Donogue, "Reasonableness in the Context of Workplace Privacy", Infonex, June 25, 2001 at p. 7.

¹³ Employers with unionized workplaces in British Columbia, depending on the circumstances, may have a statutory obligation to give notice of the introduction of a biometric system in accordance with s.54 of the *Labour Relations Code* RSBC 1996, c. 44.

input; (e) does not permit the encrypted data to be used as a unique identifier that can be used to access (or link to) other biometric information or other databases; (f) is a one-one match and does not permit biometric data from another source to be matched to the encrypted data; (f) cannot be used for any purpose other than the application for which the biometric data was collected (no secondary uses); and (g) destroys all data once it has served its original purpose will stand a better chance of success than those that do not have these features or have opposite features. In particular, the ability to reverse-engineer as was the case in *IKO Industries* or a one-to-many matching system will be problematic.

7. Develop a written policy that deals with the biometric system. This policy should explain how biometric data is collected, stored, accessed and used and specify the security controls and safeguards that are in place to protect the integrity of the data and how these responsibilities are to be discharged and by whom. It should also address how employee biometric data will be removed upon their termination, as was addressed in *Canada Safeway* and *IKO Industries*.
8. Negotiate, or attempt to negotiate a provision in the collective agreement that expressly gives management the right to introduce or implement biometric systems in the workplace or sets out a process under which this can be done. This, of course, may be impossible and the management rights clause will have to be relied upon.
9. Ensure that the biometric system does not pose any health and safety concerns (usually concerning hygiene).

V. Conclusion

Biometrics in the workplace poses a number of interesting challenges for employers and employees alike. Notwithstanding the complexity of the subject matter and the underlying technology, concerns with biometric use in the workplace should first be dealt with as a matter of common sense and secondly, as a delicate balance between the employee's right to privacy in the workplace and the employer's right to advance its business interests. In many cases, the interests will be same. In many others, it will be different. It is hoped that the above discussion will give employers a starting point for evaluating a biometric system in their workplace.