Debbie Bennett

While employers obviously recognize that employees have privacy rights, we also understand those rights are not absolute. They must be weighed against other interests that can intrude upon privacy. The objective becomes to balance privacy rights of employees against legitimate and sometimes competing interests of employers.

Employers are constantly looking for ways to improve safety and security or maximize efficiency or minimize costs – for better ways of doing things. One of the "better ways" is biometrics, which would be acceptable in some cases. Which cases depends on a number of factors. Questions an employer might want to ask include:

- What is the problem the employer is attempting to resolve through use of biometrics? For example, is the current system labour intensive, requiring substantial manual intervention? What does that labour/manual intervention cost relative to the cost of the proposed system? Is there a problem of time theft in addition to or instead of the foregoing? If on a swipe card system, are lost cards becoming costly to replace or causing a security risk? Is there a broader problem of security resulting in an attempt to prevent unwelcome visitors on company property?
- Is biometrics going to be effective in resolving these issues?
- Was the technology chosen designed with privacy objectives in mind? For example, was it one-to-one or one-to-many matching? Can fingerprints be reconstructed from the information stored in the database? What kind of firewalls are in place to prevent hacking?
- Were policies put in place to safeguard the information? For example, is it Company policy to ensure the information is stored securely, deleted immediately when no longer needed and accessed only by a limited number of individuals who absolutely require access?

- Does the employer have a policy that the information collected would only be released to external agencies, such as police, on production of a warrant or court order?
- Did the employer notify the employees/unions in advance and explain the reasons for the introduction of biometrics?
- Did the employer tell the employee/unions how the information obtained would be collected, accessed, used, disposed of and safeguarded?
- What is the law regarding use of biometrics or other process that leads to an invasion of privacy? Even if not covered by privacy legislation, consider arbitral jurisprudence and/or human rights decisions.
- Are there other statutory obligations at play?
- What does the collective agreement, if any, say?
- What practices are in place at the worksite? Is this type of data collection reasonably expected within this organization?
- What type of industry are we in/work do we do? For example, the security measures taken at the Supreme Court will be different from the measures taken at Walmart. What if you work in an industry that makes weapons or deals with matters related to national security?
- Is there a less intrusive biometric (i.e. hand scanning or voice print versus fingerprints)
- Are their special circumstances? I work with the media. Many of you who lived in Ottawa 10 years ago will remember when Brian Smith, who was a local media personality, was killed in his employer's parking lot. Media personalities are often targets, especially if their editorial stance, or perceived editorial stance, is inconsistent with the views of more radical groups, which it often is. Obviously, after his shooting, there was a heightened sensitivity, and receptiveness, on the part of employees, the employer and the unions to enhance security.
- Are there subsidiary advantages to the use of the system? In the event of a disaster which required evacuation of all employees, provided this info was backed up offsite, it could be used to alert the police/fire department that someone is missing and presumably still in the building. The same isn't as true of swipe cards given their susceptibility to time theft.