

# Consider Privacy Risks before Deploying Workplace Biometrics – Glenn Commandments



A shingle plant in Ontario wants to introduce a biometric payroll and timekeeping system that uses scanned images of employee index fingers to verify each employee's identity when they clock in and out. The union grieves. The arbitrator weighs the employees' privacy concern against the plant's legitimate business interest in a more efficient, accurate, and secure payroll and timekeeping system and finds no justification to use the biometric system when a non-intrusive swipe card system would accomplish the same goal [[IKO Industries Ltd. and U.S.W.A., Loc. 8580 \(Re\)](#), 2005 CanLII 94169 (ON LA)].

## When Workplace Security and Privacy Collide

Biometric systems use an individual's unique physical characteristics, such as a fingerprint or voice print, as a means of identification. As technology improves and costs decline, more companies are using biometric systems to perform a variety of business functions, such as in time clocks to verify employee hours and in door locks and building systems for security. But employees may consider the scanning and storing of their fingerprints, retinas, and such an invasion of privacy, as in *IKO*. To resolve these disputes courts and arbitrators balance two interests:

**Employees' Privacy:** Employees have a right to some degree of privacy in the workplace. But those rights must be balanced against the employer's right to conduct legitimate business functions. Thus, while all biometric systems invade employees' privacy to some degree, their use in the workplace isn't necessarily illegal.

**Employer's Business:** Courts consider whether the employer's use of the biometric system serves a legitimate business function. For example, the manufacturer in *IKO* claimed it needed biometric payroll and timekeeping systems to:

- Improve efficiency by reducing how much time supervisors and payroll clerks spend verifying employees' hours and calculating their pay.
- Prevent "buddy punching," a form of time theft in which one employee punches in or out for another employee who's late, leaves early, or is absent.
- Bolster security and safety by tracking the whereabouts of everybody in the plant.

## Striking the Balance

To weigh these competing interests, courts apply the rule of proportionality by comparing the importance of the business function the biometric system purports to serve against how much it intrudes on employee's privacy rights. The greater the intrusion, the more compelling the business rationale must be to justify its use. Courts also consider whether the biometric system will really accomplish the employer's goals and whether the same benefits can be realized via less intrusive methods. So, for example, even though the company in *IKO* had a legitimate business interest in using a biometric system, the arbitrator sided with the union because a less intrusive swipe card system would have accomplished the same purpose.

## 4 Things to Ask Before Deploying Biometrics in the Workplace

Before deciding to implement workplace biometric systems, employers should ask themselves four questions:

1. Will the system serve a legitimate and compelling business interest?
2. Can the company accomplish the same objectives by using a less intrusive alternative?
3. Does the biometric system have appropriate safeguards to protect the confidentiality of the personal information it collects from employees?
4. Has the company told employees about the system, how it works, the personal information it collects, how it uses that information, and what measures will be taken to safeguard the information?