Privacy: Biometrics in the Workplace

WHAT IS THE ISSUE?

Biometric information is generally a series of numbers created by a software program based on sources from your body such as fingerprints, voiceprints, iris scans, hand geometry or DNA. Biometric data can also be created from personal habits such as keystroke tapping rhythms, mouse clicks and motor skills.

Biometrics are considered to be a very reliable method of identifying people because the data is specific to one individual. While it is easy to grasp why employers may want to use biometrics, the use of such personal information may be of grave concern to the affected employees. Currently, there are few privacy law cases that involve biometric information in the workplace.

WHICH LAW APPLIES?

Privacy law for BC private sector organizations in BC, such as businesses and non-profits, are governed by the Personal Information Protection Act ("*PIPA*"). Federal works, undertakings, and businesses, such as airlines, banks and telecommunications companies, are governed under the Personal Information Protection and Electronic Documents Act "PIPEDA").

First Nations Band Councils: if you are an employee of a First Nations Band Council, the collection, use, or disclosure of your personal information is governed under PIPEDA.

Privacy law for BC public sector organizations, such as provincial government ministries and municipal police forces, in BC are governed by the Freedom of Information and Protection of Privacy Act ("FOIPPA"). Federal public sector organizations, such as federal government ministries and the RCMP, are governed under the Privacy Act.

WHAT ARE THE PRINCIPLES?

Privacy law governs the collection, use, and disclosure of personal information by balancing two principles:

- A person's right to control access to and use of their **personal information AND**
- An organization's need to collect, use, or disclose a person's personal information for legitimate and **reasonable** purposes.

- **"Personal information"** means information about an identifiable individual, including:
- Name, home address, or home phone
- Information about a person's height or weight
- Information about a person's race, religion, sex, sexual orientation, age, etc.
- Medical information
- Fingerprints, blood type, and other biometrics

Personal information **does not** include a person's contact information at a place of business.

"Reasonable" for the purposes of collection, use, and disclosure means what a reasonable person would **consider appropriate** in the circumstances.

What is considered **"appropriate"** in the circumstances will depend on:

- The amount and sensitivity of the personal information collected or used by the organization
- Whether the organization attempted a less intrusive method of collecting or using the personal information
- Whether the organization's chosen method meets its stated goal for collecting or using the personal information, such as employee safety or security

DID I CONSENT TO GIVE MY INFORMATION?

Meaningful consent is an essential element of privacy law for private sector organizations in Canada. In general, organizations are required to obtain a person's **meaningful consent** to collect, use, or disclose their personal information.

"Meaningful consent" means that a person understands the nature, purpose, and consequences of what they are consenting to. To obtain meaningful consent, organizations must make information about the collection, use, and disclosure of personal information available to the employee, including:

- What personal information is being collected
- What is the purpose for collecting, using, or disclosing the personal information
- With what other parties will the personal information be shared

Note that employers may collect, use, or disclose personal information for the purposes of establishing, managing, or terminating the employment relationship.

LAW ON BIOMETRICS

If you are a unionized employee, you may be able to rely on the collective agreement that governs your employment if it has applicable provisions. You may also look to decisions by labour arbitrators and judges with respect to unionized workplaces to see how similar matters were determined.

There are few cases that involved the collection or use of biometric information in the workplace. To date, there are no decisions by BC's Office of the Information and Privacy Commissioner on the subject. However, Alberta's Information and Privacy Commissioner dealt with a complaint filed by an employee who did not want to scan her thumbprint as required by a new sign in system installed by her employer. It was determined that the biometric timekeeping system was necessary for the employer as the previous punch card system enabled employees to access one another's timecards and to sign them in even if they were late or absent for work.

WHAT CAN I DO ABOUT IT?

If you believe your employer has breached your privacy rights, you can take the following steps:

1. Request your employer's privacy policy. If you are in a unionized workplace, also consult your collective agreement.
2. Attempt to resolve your concerns directly with your employer. Keep records of your correspondences with your employer.
3. If you are unable to resolve your concerns, you can file a formal complaint with the provincial or federal privacy commissioner.

For complaints under PIPA or FOIPPA, you can file a complaint with the Office of the Information and Privacy Commissioner for BC. You can call the OIPC at (250)-387-5629.

For complaints under PIPEDA or Privacy Act, you can file a complaint with the Office of the Privacy Commissioner of Canada. You can call the OPC at 1-800-282-1376.

If your complaint is accepted, a file will be opened and you will be sent a notice with a file number. In processing your complaint, the Commissioner may do one of the following:

- **Mediation:** An investigator will attempt to settle the complaint between you and your employer. No finding will be issued.
- **Investigation:** An investigator will conduct an investigation into the complaint, which will include gathering statements and evidence. A report will be issued with a finding of whether or not your employer breached the applicable privacy legislation.

The Commissioner cannot impose fines or awards for damages against your employer. The Commissioner can issue a directive for your employer to comply with the applicable privacy legislation.