Should You Fingerprint Scan Your Employees?

Biometric Information In Today's Workplace

Fingerprints, handprints, facial features, voiceprints, iris scans; are you ready for the collection and storage of biometric data from your employees?

What you should know about the collection of biometric data from employees in Canada

How comfortable are you with the idea that your employer may be collecting and storing a copy of your fingerprints? With the announcement of the new Apple IPhone's fingerprint id, we are getting one step closer to the routine use of biometric scanning in every workplace.

Biometric scanning is a convenient way to monitor and gather information on employee activities. Biometric scanning is already used in some workplaces to confirm employee's identity. Identity confirmation is necessary for employees to gain access to the workplace and restricted areas, confirm entitlement to services, and monitor and record their activities. Using secure, personal information can increase security and reduce unwanted access in the workplace. Another benefit of biometric data is that employees cannot lose or forget their 'id' or easily transfer it to someone else. Like all other personal data, however, there is a risk that others may steal and misuse this data and, in fact, it is not impossible at all to transfer the data to someone else.

Canadian privacy regulations are trying to stay on top of this trend by attempting to ensure your information is collected and stored appropriately. Collection of this data falls under PIPEDA (Personal Information Protection and Electronic Documents Act). PIPEDA is a federal private sector statute covering most provinces (British Columbia, Alberta and Quebec each have their own privacy statutes).

Clarify Why You Are Collecting the Information

In order to gather information via biometric scanning, you need to ensure the reasons you are collecting it are reasonable and appropriate. To help determine this, you need to be aware of both the relevant Canadian requirements and your local Provincial ones. For example, the employer must consider if the business objectives are legitimate and bonafide and effective in meeting the objectives for which they are being gathered. There is still a lot of grey area here, so, before you collect this data, decide if it is really worth the time, resources and potential risk.

Notify Employees About Biometric Screening

Before you collect any biometric data you must:

1. Notify employees in writing about the mechanics of biometric collection and clarify what personal information is collected and how it will be used and secured.
2. Ensure your organization's privacy policy includes reference to the collection, use, disclosure, security and retention of biometric information
3. Provide all current and any new employees with a copy of your organization's privacy policies.

Consider What Biometric Information Is Collected And How It Will Be Stored

Right now it is not uncommon to use facial recognition, in photos, to identify employees. Photos may be part of a swipe card technology or worn on a badge. Collecting photos and having a person 'eyeball', or compare, them to a database is the most basic collection of biometric information. If you store the photo of the person in a computer file somewhere and this photo is used to compare to the person or person's photo, then you are storing a 'literal' representation of personal data in your system. If you have all the photos of your employees held in your system, and when an employee signs in, you match him or her to a photo in your database, this is called a "one-to-many" comparison. The process is similar to what is portrayed by TV on procedural shows such as NCIS or CSI. This comparison process is currently the most common and least 'secure' way of collecting, securing, and using individual identification information. The method of literally storing biometric data, whether that is a photo, fingerprint, voiceprint is insecure because the literal information that can be taken and used elsewhere.

Technology that enables you to gather biometric data but not store it in its literal representation also exists. This technology is often called 'untraceable' biometric data. Using untraceable biometric data allows for one-to-one matching by translating personal information into a numerical representation of the data, which is then used for direct authentication. This stored biometric data cannot be reconstructed or reproduced. In this case, an employee presents their 'live sample', their face or fingerprint, and this information is translated into a numerical code which is then compared to the stored code of information. According to reports, Apple's new IPhone does not store a literal representation of the fingerprint data but a numerical one, which is encrypted and used to compare against the fingerprint applied for access.

Privacy Concerns

Each day we are tagged by biometric data whether you are aware of this or not. If you recall the 2002 Tom Cruise movie, 'Minority Report' you would have seen the use of facial recognition and iris scan data everywhere to allow access and track behavior. Facebook scans photos you upload and asks you to tag faces (thus, it learns to recognize faces). When you enter some retail stores, these stores use technology to identify your face (or your phone) and connect that to past shopping preferences. These trends raise significant privacy concerns that will shape the collection and use of data in the next few years.

Today, if you are choosing to gather biometric data, you must notify your employees. You also need to be certain that you are gathering it for the right purposes and storing the data appropriately once collected.