CLOCKING IN AND OPTING OUT: QUEBEC CAI ISSUES WARNING ABOUT BIOMETRIC TIME CLOCKS IN THE WORKPLACE

Posted on May 24, 2023

Categories: Insights, Publications

Organizations considering tracking their employees' time using biometrics in Québec must tread lightly.

On March 27, 2023, Québec's privacy regulator, the *Commission d'accès à l'information* (the "CAI") published its observations (available in French only at this time) on the increasing trend among organizations to use biometric time clocks to monitor and manage employee hours and payroll. The CAI highlights that, in most cases, organizations' use of biometric time clocks does not comply with applicable privacy legislation.

Biometric time clocks are devices used to identify employees and track their work hours using an employee's biometric information, such as fingerprint, palm, facial or iris scan. Biometric scans are generally considered by employers to be quick and reliable means for tracking employees. Unlike access cards or entry codes, an employee's biometric information cannot be borrowed and swiped by other employees, nor can it be forgotten or misplaced. However, since biometric data is "distinctive, unlikely to vary over time, difficult to change and largely unique to the individual",[1] it is also considered highly sensitive.

To mitigate risks to your organization from possible complaints and fines associated with the misuse of biometric information, it is important for organizations to stay up to date on requirements set out in legislation and CAI guidance. This bulletin provides a guide to the legislation and CAI guidance surrounding biometric time clocks in Québec.

1. Legal Requirements Prior to Establishing a Biometric Database

In Quebec, the *Act to establish a legal framework for information technology* requires that the creation of a biometric feature or measurement bank for the purposes of identification or authentication be disclosed to the CAI no later than 60 days before it is put into service. Organizations are therefore required to make a timely declaration to the CAI regarding the use of biometric time clocks.

Consent must be obtained from employees prior to collecting biometric information or implementing a biometric system. In particular, the CAI has published a consent template (available in French only at this time) which organizations can use and adapt to their own specific needs. Organizations must provide consent forms

containing all the necessary information to their employees to obtain their express consent which must be free, informed and specific and time-limited.

Importantly, the CAI reiterates that, even where consent is obtained from employees, an organization must be prepared to demonstrate why it was necessary within the meaning of the *Act respecting the protection of personal information in the private sector* to implement and use a system that collects biometric information. In other words, consent is not a substitute in the absence of necessity.

2. Two Criteria to Determine if Your Use of a Biometric Database is Compliant With the Law

Is the Purpose Important, Legitimate and Real?

When deciding whether to establish a biometric database, organizations must first determine if their purpose for doing so is important, legitimate and real. Organizations must undertake an assessment of the circumstances and issues that led to the decision to implement a biometric time clock.

The CAI has indicated that typical management objectives (e.g., desire to improve the efficiency of payroll management through automation, to use the same system as other branches of an organization, to avoid loss and breakage of magnetic access cards, etc.) generally do not reach the level of importance to justify the collection of such sensitive information. Similarly, concerns of potential problems, such as time theft, also fail to meet this first criterion. The CAI will look for real and documented evidence of a serious issue that cannot be resolved without resorting to biometrics.

Organizations must ensure that this assessment is well documented. In case of a complaint or investigation by the CAI, this will allow the organization to demonstrate that it has carried out a rigorous assessment and meets the above-mentioned criteria.

Is the Collection Proportional to the Purpose?

Where an organization concludes that its purpose for collecting biometric data is important, legitimate and real, it must determine whether the method of collection, along with the proposed data to be collected, is a proportionate means of achieving that purpose.

According to the CAI, for the collection of biometric information to be a proportionate means of achieving the organization's purpose:

i. the use of a biometric time clock must be an effective way to achieve the objective (rational link);
ii. less intrusive means of achieving the desired objective must be given priority, minimizing collection in the absence of other means; and
iii. the benefits of using a biometric systems must outweigh the infringement of employees' rights and the

adverse consequences that may result from the implementation of such system.

The CAI observes that in practice, organizations rarely consider or document the possibility of using less intrusive means. Furthermore, organizations frequently fail recognize or mitigate the impact on employee privacy, or minimize the collection of biometric information to just what is necessary.

Where all of the proportionality criteria are met, organizations must finally respect the right of employees to refuse to have their biometric information collected by seeking express consent and providing an alternative to the use of a biometric time clock. This is considered a key element of free consent by the CAI as illustrated in its Draft Consent Guidelines published on May 16, 2023.

Issues in Practice

Two decisions rendered by the CAI in 2022 illustrate the above principles.

In a decision regarding a regional hotel,[2] biometric information was being used for payroll processing. The CAI found that, even if the data collected by biometric time clocks is converted into mathematical code, it continues to be considered personal information because it is unique to the individual and allows for identification.

In this case, the hotel's objective for implementing the biometric time clock system was to improve the efficiency of payroll processing. The Company estimated that it saved over 400 hours per year by switching to the new biometric system. While the CAI agreed that the purpose was legitimate and stemmed from a real problem, it nevertheless concluded that the organization did not demonstrate that this purpose was sufficient to justify the collection of biometric information. The CAI considered that the improved efficiency of the payroll system, which is a common and intrinsic objective in the management of any company, was not sufficient on its own to demonstrate necessity.

The CAI also found that, even if the purpose were sufficiently important, the invasion of privacy was disproportionate to that purpose, given the sensitive nature of biometric information. The CAI also noted that alternative software existed, which could automate the processing of payroll without collecting biometric information. Accordingly, the CAI ordered the organization to cease its collection and to destroy the data it stored.

In a similar decision,[3] after the CAI's inquiry, an organization failed to demonstrate how the invasion of privacy was minimized or how the benefits of the biometric time clock outweighed the significant invasion of employee rights. The organization decided to stop the use of the biometric time clock and destroyed all biometric information it had collected.

3. Consequences of Failing to Comply with the Legislation

Failing to comply with the legal requirements and the CAI's guidance will expose organizations to serious financial consequences.

As presented in greater detail in our bulletin titled Bill 64 Enacted: Québec's Modern Privacy Regime, further to amendments brought by the *Act to modernize legislative provisions as regards the protection of personal information*, the CAI will, as of September 22, 2023, have the ability to impose significant administrative monetary penalties of up to $10,000,000 or 2% of the organization's worldwide turnover to any organization in contravention of applicable laws. In addition, albeit reserved for egregious offenses, the CAI will also be able to impose penal fines up to the greater of $25,000,000 or 4% of the organization's worldwide turnover.

Aside from these penalties, the CAI can, on its own initiative or pursuant to the complaint of an individual, conduct an investigation into an organization if it suspects that it does not comply with the law. Furthermore, individuals can now bring a private action against an organization for damages resulting from the unlawful infringement of the right to privacy. When such an infringement is intentional or results from gross negligence, the victim would be entitled to punitive damages of at least $1,000.

4. Steps for Compliance

In summary, in addition to the requirement to give notice to the CAI, before implementing biometric time clocks or similar systems using biometric information in Québec, organizations must:

- Identify the purposes for the implementation of such devices or systems;
- Document any problematic situations to be remedied by their implementation;
- Assess the situation and ensure that the defined objectives are real, legitimate and important enough to justify the collection of sensitive biometric information;
- Ensure that there are no other, less intrusive means to achieve the objectives (and document this analysis);
- Weigh the benefits along with the impact on employees including the risks of their biometric information being compromised;

If the organization concludes that the collection of biometric information is necessary within the meaning of the law, it must also:

- Ensure that the chosen system minimizes the invasion of privacy, provides appropriate safeguards and complies with other legal obligations; and
- Provide an alternative means to employees who do not wish to identify themselves using biometric information.

As recommended in the CAI's Companion Guide for the use of biometrics, carrying out a privacy impact assessment will allow the organization to consider and document the above criteria in a rigorous manner. Privacy impact assessments will become mandatory as of September 22, 2023 for any project to acquire, develop or overhaul an information system or electronic service delivery system involving the collection, use, communication, keeping or destruction of personal information.

McMillan is happy to assist with any specific advice on navigating your obligations under the Québec privacy regime.

[1] See PIPEDA Report of Findings #2021-001: Joint investigation of Clearview AI, Inc., by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information and Privacy Commissioner of Alberta, February 2, 2021, available online.
[2] Decision of the Commission d'accès à l'information du Québec, Auberge du lac Sacacomie inc., available online.
[3] Decision of the Commission d'accès à l'information du Québec, Enquête à l'égard de Compagnie Selenis Canada, available online.

by Alice Ahmad, Ayse Gauthier, and Robbie Grant

A Cautionary Note