Are Canadian Employers Crossing the Line Without Realizing It When It Comes To Biometrics and Privacy in the Workplace?

A few years ago, fingerprint scanners and facial recognition cameras sounded like science fiction. Today, they're quietly showing up in the most ordinary places. Employees clock in with a thumbprint, unlock doors with a facial scan, and verify attendance using voice recognition. The promise is efficiency and security. But in Canada's legal landscape, that promise comes with a catch: these same technologies carry enormous privacy and human rights implications that many HR teams are only beginning to understand.

Across the country, privacy commissioners are increasingly sounding the alarm. What started as a convenience tool in corporate offices and retail stores is now becoming a compliance risk. The line between safety, surveillance, and privacy has never been thinner, and HR professionals are suddenly on the frontlines of that debate.

A New Frontier for Workplace Data

Canadian workplaces already handle deeply personal information—salaries, health data, performance records, and even background checks. But biometric data is different. It isn't just another record in a file. A fingerprint, an iris scan, or a voiceprint is a permanent identifier of who someone is. You can change a password, but you can't change your fingerprint if it's stolen.

That permanence is what makes biometrics such a powerful tool for safety and access control, but it's also what makes it uniquely dangerous when mishandled. The Office of the Privacy Commissioner of Canada (OPC) classifies biometric information as "sensitive personal data" because of its potential for misuse. It's not just data theft at stake—it's identity theft of the most personal kind.

And yet, because biometrics are so easy to implement through off-the-shelf tools, companies across Canada are adopting them faster than they can evaluate the risks. From construction sites tracking attendance to healthcare organizations verifying staff access, the technology is everywhere. For HR managers, that means the time to understand the rules isn't tomorrow — it's right now.

The Patchwork of Privacy Laws

Unlike Europe's General Data Protection Regulation (GDPR), Canada doesn't have a single, all-encompassing law dealing with biometric data. Instead, there's a patchwork of rules that vary by province and by sector. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) sets broad principles for how personal information is collected, used, and disclosed in commercial activities. It treats biometrics as personal information but doesn't spell out specific biometric rules.

The real action is happening at the provincial level, where privacy commissioners have been far more assertive. Québec, for example, treats biometric data as inherently sensitive and requires organizations to justify why they're collecting it. Employers must prove that no less intrusive method could achieve the same purpose. Québec's privacy authority, the Commission d'accès à l'information (CAI), also requires businesses to notify the Commission before creating any biometric database. Companies that skip this step can face suspension orders or investigations.

British Columbia and Alberta have their own private-sector privacy laws deemed "substantially similar" to PIPEDA. They too recognize biometrics as personal information and emphasize the need for meaningful consent. But they also add an extra layer of complexity—especially in the employment context, where consent can be hard to prove as "voluntary" because of the inherent power imbalance between employers and employees.

For HR leaders, that means a fingerprint scanner in Vancouver might trigger different legal requirements than the same system in Montreal or Calgary. And if your organization operates nationally, you could be dealing with three or four privacy regulators at once.

When Security Meets Surveillance

The original intent behind most biometric systems in the workplace is sound. Employers want to ensure that only authorized individuals can enter certain zones, handle sensitive materials, or access hazardous equipment. But technology that starts as a safety measure can quickly drift toward surveillance.

In one British Columbia case, a group of small retail stores under a national banner installed facial recognition cameras to deter shoplifters. The system captured every customer's face and compared it against a database of "persons of interest." The privacy commissioner found the practice unlawful because the stores had not obtained meaningful consent from customers. Even though the intention was to protect staff and property, the indiscriminate collection of biometric data crossed the line.

A similar issue arose in Québec, where a printing company deployed facial recognition for workplace security. The CAI ruled that the system was unnecessary and disproportionate to the goal. The company could have achieved the same security results with less intrusive measures, such as access cards or ID badges. Consent alone, the Commission said, was not enough to justify the invasion of privacy.

These decisions reflect a broader principle in Canadian privacy law: even if an individual agrees to provide biometric data, the organization must still prove the collection is necessary, proportionate, and reasonable. Consent doesn't make every data use acceptable.

The Human Element

Imagine being a warehouse employee told that your new time clock requires a handprint to log your shift. You might hesitate, but you also might not feel you have a choice. In employment relationships, that’s the core ethical dilemma. True consent requires freedom, but freedom is hard to claim when your job depends on it.

This power imbalance is exactly why several Canadian privacy commissioners have warned against overreliance on consent in the workplace. They’ve urged employers to consider alternative approaches that don’t require biometric collection or to provide an equivalent, non-biometric option. HR departments that fail to offer a choice risk more than a complaint—they risk eroding trust among their workforce.

Trust is hard to rebuild once it’s lost. Employees are more data-literate than ever. They know about breaches, surveillance, and misuse of personal information. When they feel watched or tracked, even for legitimate reasons, morale suffers. That’s why clear communication about purpose, safeguards, and employee rights is crucial. Biometrics shouldn’t be a surprise announcement; it should be a dialogue.

What Happens When Things Go Wrong

In 2020, Canadian headlines were dominated by the Clearview AI scandal. The New York–based company had scraped billions of images from social media platforms and used them to power facial recognition software marketed to law enforcement. Several Canadian police services used the tool without public knowledge. The OPC later ruled that Clearview’s actions violated Canadian privacy laws. The company was ordered to stop collecting and using Canadians’ biometric information.

Although Clearview AI wasn’t a workplace case, it changed the national conversation about biometrics. It revealed just how easily personal data can be harvested, stored, and shared across borders without consent. It also underscored that Canadian authorities are willing to take a hard stance against biometric misuse.

A more recent case in Québec involved a major grocery chain that proposed installing biometric payment systems at self-checkouts. Customers could pay simply by scanning their faces. The CAI blocked the project, finding that the company failed to demonstrate necessity and had not provided adequate consent mechanisms. Again, the intention—convenience—was not enough to justify the collection of highly sensitive data.

Both examples send a message: innovation is welcome, but privacy must come first. Organizations that treat biometric data as ordinary information will find themselves on the wrong side of public opinion and the law.

The Growing Risk of Data Breach

Every HR professional knows the pain of a data breach—an employee’s Social Insurance Number exposed, a payroll system hacked, or medical records leaked. But a breach involving biometric data is in a league of its own.

Passwords can be reset. Credit cards can be reissued. But biometric identifiers are unchangeable. If a hacker obtains a copy of a facial template or fingerprint hash, that individual’s identity is compromised forever. The Canadian Centre for Cyber Security has warned that biometric systems must be treated as high-value targets and designed with rigorous encryption and limited retention. Storing biometric data indefinitely or in raw form is asking for trouble.

The cost of such a breach is not just legal—it's reputational. Consumers and employees are increasingly choosing where to work or shop based on how companies handle privacy. A 2023 Cisco study found that over 80% of Canadians consider how organizations use their data before making purchasing or employment decisions. For HR departments that work hard to cultivate an employer brand of trust and respect, a privacy failure can undo years of goodwill.

The Bias Question

There's another, more subtle risk that HR managers can't afford to overlook: bias. Many facial recognition and biometric systems have been shown to perform unevenly across demographics. Studies from MIT and the U.S. National Institute of Standards and Technology (NIST) found that some facial recognition algorithms misidentified darker-skinned individuals and women at rates far higher than white men.

If such a system is used for workplace access or attendance, it could result in real harm—denied entry, incorrect time logs, or even unfair disciplinary actions. In the worst cases, these errors could amount to discrimination under Canadian human rights law. The Canadian Human Rights Act prohibits practices that adversely affect employees based on race, gender, or other protected grounds. A biased algorithm, even if unintentionally discriminatory, could put an employer in violation of that law.

Bias is not an abstract problem. In 2022, a Toronto tech company tested a facial verification system for its office entry. It worked well for most staff but frequently failed to recognize employees of South Asian descent, locking them out or forcing repeated scans. The issue wasn't deliberate discrimination; it was a design flaw in the algorithm's training data. But the impact was the same—humiliation, frustration, and a wave of complaints to HR. The company scrapped the system within weeks.

This is where HR's voice is essential. When technology affects fairness, inclusion, and dignity, HR must be part of the decision-making process. A security tool that undermines equity is not a success—it's a compliance nightmare waiting to happen.

The Vendor Problem

Most organizations don't build their own biometric systems. They buy them. That creates another layer of risk. Vendors may store data on cloud servers outside Canada, where different privacy rules apply. They may also collect more information than necessary or keep it longer than agreed. In Québec, any biometric database must be declared to the CAI, but if your vendor hosts it, you might not even know where it resides.

Due diligence is critical. HR and procurement teams should collaborate to vet vendors not just for functionality but for privacy posture. Are they compliant with PIPEDA and provincial laws? Where is the data stored? Who has access? What happens when the contract ends? Too often, organizations discover these answers only after a complaint or investigation.

Why This Matters for HR

At first glance, biometrics might seem like a technology or legal issue. But it's deeply human. HR professionals are the custodians of trust within an organization. Employees look to HR to safeguard their personal information and advocate for their rights. If HR doesn't understand the implications of biometric collection, no one else will connect the dots between policy, ethics, and lived experience.

In workplaces where safety and security are paramount—such as healthcare, manufacturing, or critical infrastructure—biometric systems may have a legitimate role. But even there, they must be proportionate. A fingerprint scanner to prevent unauthorized access to a chemical storage room might be reasonable. A facial recognition camera tracking everyone's movements throughout the day is not.

This is where HR's influence becomes strategic. HR can help shape policies that balance operational needs with privacy principles. By bringing privacy experts, legal counsel, and IT security to the table early, HR ensures that biometric tools serve people, not the other way around.

Lessons from the Courts and Regulators

In Canada's evolving privacy landscape, decisions from regulators are providing valuable roadmaps for HR leaders. Consider the 2021 findings of Québec's Commission d'accès à l'information regarding a security company that collected fingerprints for workplace access. The CAI concluded that the system was excessive because the company had not demonstrated that less intrusive alternatives were inadequate. Even though employees had technically "consented," the consent was invalid since it wasn't free and informed. The company was ordered to dismantle the system and destroy all biometric data.

Another example comes from the British Columbia Office of the Information and Privacy Commissioner, which found that a major retailer's use of facial recognition in stores violated the province's privacy laws. The commissioner emphasized that the company's signage – "This area uses video surveillance for security purposes" – did not count as informed consent for biometric collection. Customers were never told that their unique facial features were being recorded and analyzed.

Each of these rulings reinforces a key principle: in Canada, necessity, transparency, and proportionality are not optional. They are the foundation of lawful biometric use.