Consider the Legal Ramifications Before Deploying AI for HR Functions: The Glenn Commandments

Guess what? Companies can actually use artificial intelligence to carry out HR functions.

OK, maybe you already knew that. But there are also things about using AI for employment operations that not every single HR director on the planet has heard about. One of them is how the most elaborate and state-of-the-art technology solutions that your IT people architect can be undone by legal glitches that nobody foresees.

Arbitrator Orders Bus Company to Stop Using Invasive AI Driver Monitoring System

A Montreal bus company recently learned this lesson the hard way. **Picture this:** The company invests what must have been a small fortune to replace its in-vehicle surveillance cameras with an elaborate AI-based system equipped with a G-force sensor capable of detecting sudden braking or acceleration, sharp turns, collisions and speeding, and other unsafe driving behaviours. There's also an interior camera to detect cell phone use, inattentive driving, and failure to wear a seatbelt. Upon detecting a triggering incident, the system also generates a 2- to 10-second video clip that management can later review. Although it's not cheap, the company believes that the new system from the U.S. company Samara, will generate safety improvements that more than offset the costs of deployment.

What the company apparently fails to consider is the push back from within. While the drivers and their unions have been willing to accept monitoring for safety purposes, the Samsara remote driving system is far more intrusive than the old surveillance cameras. So, the union files a grievance claiming that the new system violates their Charter privacy rights.

The company insists that the union's legal claim is bogus, but the federal arbitrator disagrees. The monitoring capabilities of the new system go beyond safety by subjecting drivers to surveillance of private activities, the arbitrator reasons, noting that video recording begins as soon as the driver starts the vehicle alone at the garage and continues for up to 15 minutes after the engine is switched off. "This

makes it possible to monitor drivers' comings and goings, including during breaks." **Result:** The arbitrator orders the company to stop using 4 features of the Samara system that intrude on the drivers' privacy rights within 90 days:

- Remote live access.
- The retention of video surveillance tapes from the interior camera not linked to reported security incidents with discretionary access for people designated by the employer.
- The publication on the vehicle location page of the driver's photo updated every 2 minutes.
- The dissemination within the company of videos of incidents involving the unit's drivers when those drivers are identifiable.

Adding insult to injury, the arbitrator also orders the company to pay $100 in privacy damages to each driver affected by the new system [*STT de Coach Canada – CSN v Newcan Coach Company ULC (Coach Canada*), 2025 CanLII 96672 (CA SA), August 29, 2025].

Takeaway

Let the *Coach Canada* case serve as a reminder that the AI systems you deploy to solve HR challenges may also expose your company to liability risks that you don't expect. One of those risks is invasion of employee privacy rights. As in *Coach Canada*, the problems often arise with AI, ChatGPT, and other digital monitoring technologies that gather and analyze detailed data on what employees are actually doing and not doing while performing their jobs.

Ontario has actually adopted a law specifically addressing this issue—erstwhile Bill 88, which amends the Employment Standards Act to require employers to implement a written policy disclosing to the employees they use AI to monitor:

- The electronic monitoring devices they use.
- The information those devices collect.
- How the company uses the information it collects.
- The third parties to which it discloses that information.
- The purposes of using such devices.

Other recommended best practices for guarding against AI privacy risks and ensuring that what happened in *Coach Canada* doesn't happen to you:

1. **Limit Use to Safety Purposes**

Privacy-invasive AI is easier to justify when its purpose is to ensure health, safety and security, as opposed to enhancing productivity. Even so, employers must still show that:

- The use of the AI or other technology is "demonstrably necessary" to meet the safety need.
- The technology is likely to be effective in meeting that need.
- The loss of employees privacy is proportional to the benefit gained.
- There are no less privacy-invasive ways of achieving the purpose.

2. **Keep Information Collected to a Minimum**

Collection must be limited only to personal information necessary to accomplish the purpose of deploying the technology and not include non-work-related personal information in which employees have reasonable expectations of privacy. Accordingly,

AI software or apps that tap into employees’ personal calls, emails, or computers are highly problematic, as is spyware and other technologies for secretly monitoring employees without their knowledge.

3. **Consider Need for Consent**

You generally need consent to collect, use or disclose employees’ personal information unless:

- Getting consent would compromise the availability or accuracy of the information collected.
- Collecting information is for the purpose of investigating violations of the law or employment agreement.