Watching Out For Privacy: Limitations On Employer Video Surveillance

In *Rehn Enterprises Ltd.* v. *United Steelworkers, Local 1-1937*, 2024 CanLII 72130 (de Aguayo), Arbitrator Jacquie de Aguayo found numerous privacy and procedural breaches related to the installation of video surveillance in work vehicles.

Background

Employees at Rehn Enterprises Ltd. (the "**Company**") perform hand-falling work in the forestry industry. Their work involves 2 to 3 paid hours of commuting per day in Company-owned vehicles (the "**Vehicles**").

In February 2023, the Company installed dash cams in the Vehicles. The cameras, which were located at the front of each of the Vehicles by the rearview mirror, continuously recorded both forward and rear-facing video, audio and GPS data, including video and audio from inside the Vehicles while in use. The data was then uploaded to a third-party platform where it was stored until it was overwritten. The platform used an AI program to analyze the recordings and generate "safety alerts" ("**Alerts**") based on criteria set by the Company. At the time of the grievance, the Company's safety criteria included driver cellular telephone usage, failure to wear a seatbelt, speeding, insufficient following distance, harsh breaking, collisions, near misses, hard turns and obscuring of the camera.

If an Alert was generated, a picture with embedded video and GPS data was stored indefinitely on the platform. Company-authorized individuals would view the recordings generated after an Alert and were then required to decide whether the recording showed an infraction that required coaching or discipline.

Grievance

The Union grieved the installation of the cameras in March 2023 as breaches of employee privacy rights. Although the Company did not roll out a policy regarding the cameras until September 2023, the parties agreed to include the policy in the grievance (the "**Policy**").

The primary issue at arbitration was whether the surveillance during paid travel time was a reasonable exercise of management rights and whether it appropriately balanced the employees' privacy rights. The Union did not take issue with the GPS recordings or front-facing cameras while the Vehicles were in motion and accordingly, the

arbitration primarily considered the rear-facing video and audio recordings and front-facing recordings during idling time only.

Analysis

Arbitrator de Aguayo's analysis was conducted against the backdrop of the *Personal Information Protection Act*, S.B.C. 2003, c. 63 ("***PIPA***"), the legislation governing the privacy obligations of private organizations in British Columbia, and the arbitral jurisprudence around surveillance. The overriding consideration was whether the Company's safety interests were appropriately weighed against the employee's privacy interests.

Arbitrator de Aguayo assessed the following relevant factors: (i) whether the concern for safety and security was *bona fide*; (ii) whether there was a direct link between the camera installation and the safety and security issues, including whether there was evidence that the cameras were for reasons other than safety or security; (iii) the manner in which the surveillance was implemented, including the reasonableness of the number of cameras, the place of installation and the use of the footage; and (iv) whether there were alternatives to address the safety and security concerns.

The arbitrator found that the privacy interest at stake was high – there was a significant collection of personal information – and while a genuine safety concern existed for employees driving on logging roads, there was no evidence to show that safety was an unusual risk beyond the normal high-stakes nature of driving in remote areas. Further, the circumstances in which recordings could be viewed were broad and the AI system that was used to create Alerts did so frequently and at times in error. Such Alerts might relate to genuine near misses or accidents but could also show the employee doing something such as vaping which would then become the focus of an investigation and potential discipline (not safety-related).

Ultimately, Arbitrator de Aguayo concluded that the surveillance was unreasonable because the rear-facing cameras had only a speculative and tenuous link to safety. Based on the evidence, she found that the primary purpose of the rear-facing cameras in this case was to send a message to the employees that they were being watched and to serve as a tool to investigate employees' potential misconduct (not a means of determining the cause or circumstances of genuine safety events).

The arbitrator characterized the surveillance as an overzealous exercise of management rights. She noted how "if a direct link to safety or the reasonable use of the Surveillance turns on technology's ability to open up potentially relevant lines of inquiry to find an 'incident', or constant surveillance can alone modify behaviour, employees' informational privacy rights would be illusory in virtually every case".

She further found the Policy to be unreasonable due to breaches of *PIPA*, including insufficient notice to employees, indeterminate and unreasonable storage length of information, and an absence of procedures in the event of a security breach or a lack of Company efforts to ensure security of data.

Arbitrator de Aguayo upheld the grievance and ordered the Company to immediately turn off the rear-facing cameras, delete stored footage and revise the Policy and collection of personal information to comply with her award. She also ordered the Company to pay $4,000 in general damages to each employee as a breach of their privacy rights.

Takeaways for Employers

Employers have the responsibility to maintain safe workplaces and this can, in some circumstances, justify the use of surveillance. However, given the significant intrusion on employee privacy, employers should be cautious and measured in their approach, including by:

- considering whether other measures can address the safety risk in question;
- limiting the intrusion to what genuinely addresses the safety risk;
- following all legislative requirements to ensure data protection and privacy when collecting employee personal information;
- rolling out the surveillance in a way that gives employees sufficient notice and clear information about what information is being collected, how it is stored and how it will be used.

Originally published by LexisNexis Labour Notes Newsletter.

Authors: Julia Bell, Andrew Hefford

Roper Greyell LLP