STOP SNOOPING: ALBERTA PRIVACY COMMISSIONER FINDS EMPLOYEE SNOOPING RESULTS IN REAL RISK OF HARM

Posted on September 21, 2022

Categories: Insights, Publications

In a recent breach notification decision, the Alberta Privacy Commissioner found that a real risk of significant harm arose after four employees were found to have accessed account information of other employees and credit union members without an authorized purpose. This decision highlights the importance of clear privacy policies and practices for employees and that the risk of privacy breaches is not just from external bad actors – it can arise inside of an organization.

Background

The organization discovered this breach through their internal audit system shortly after the unauthorized accesses occurred. It involved sensitive personal information of employees and credit union members, including their social insurance number, banking information, and other sensitive employment information.

Under the Alberta *Personal Information Protection Act*,[1] organizations are required to notify individuals if unauthorized access of their personal information raised a real risk of significant harm. This test was met due to the sensitive nature of the information accessed and the deliberate and personal nature of the breach, together with the non-trivial consequences or effects of the incident. The decision also noted how, because the perpetrators and affected individuals know each other, there was an increased likelihood that this incident would damage personal and professional relationships.

Organization's Response

As a result of this breach, the organization provided the necessary access notification[2], offered the affected individuals 24 months of credit monitoring, and took several steps to prevent future breaches including:

- Disciplining the employees who conducted the accesses;
- Developing a "spot check" program to monitor employee accesses; and
- Reminding all employees of the audit tool, the importance of maintaining privacy, and the consequences of a failure to do so.

These steps were aided by the fact that the organization had these processes and policies in place before the

breach.

Takeaways for Businesses

This decision serves as a reminder for all businesses to have clear policies and practices in place – such as an employee privacy policy, an internal audit process, and proper safeguards on employee personal information. These not only reduce the risk of a breach, but also allow for a quick and effective response if a breach occurs, in order to reduce the risk of harm to individuals.

For more information on Alberta's regulation of privacy breaches, please see our recent bulletin, Lessons learned from Alberta's Office of the Information and Privacy Commissioner (OIPC) 11-Year Report.

If you would like advice on drafting or revising such policies or procedures, or employee privacy considerations more generally, a member of our Employment & Labour Relations Group would be happy to assist you.

by Gordana Ivanovic, Kristen Shaw and Julia Loney

[1][ps2id id='1' target=''/] *Personal Information Protection Act*, SA 2003, c P-6.5, s 37.1.
[2][ps2id id='2' target=''/] Required under section 19.1 of the *Personal Information Protection Act Regulation*.

A Cautionary Note