Don’t Gather Your Employee’s Personal Passwords

Alberta Privacy office finds employee’s personal email password is private.

It should be obvious that an organization should not take the password of an employee’s personal email and use it to monitor the employees communications. Often, however, employees do not know about or even consider where their organization’s right to monitor employee activities cross the line. Recently, the Alberta Office of Information’s Privacy Commissioner issued a sanction against an employer, Moore’s Industrial Service LTD, for breaching the privacy of a former employee.

In this specific situation, the terminated employee complained that his former employer had accessed his personal emails by obtaining his personal password from a company laptop. Furthermore, he presented information confirming his former employer used personal information to access ongoing personal email communications after the employee had been terminated. The organization claimed they had implicit rights to access information found on the company owned laptop because the employee consented to access by putting his personal password on the laptop. What do you think crosses the line?

No Right to Use The Employees Personal Email Password

In this case the Alberta Commissioner Adjudicator found that a person’s personal password and email account information are considered ‘personal’ for the purpose of PIPA (Personal Information and Protection Act) and that the employer did not have a right to access this information.

The employer argued that the information accessed was relevant to ensuring the employee conformed to post-termination agreements. The adjudicator, however, concluded there was no reason or basis to suspect a violation of the agreement and, as a result, on-going surveillance was not justified. Furthermore, the adjudicator indicated that even if there was reason to believe the employee was violating a post-employment agreement, it would most likely not justify their ongoing monitoring of his personal email correspondence.

The adjudicator also noted that the employers continued access to the personal information and email of the former employee was far from being okay and was “excessively invasive and patently unreasonable”.

What Does This Mean About Company Computer Privacy?

It is important for organizations to ensure their computer use policies are clearly spelled out and understandable to their employees. In this case, even a policy that says the employer could access and use personal information found on a company computer does not justify the employer’s actions.

It is important to ensure adequate training of all employees both in storing their personal information and removing their personal information when returning company property. Training all employees on what constitutes personal information and what information they must not access or share would be a prudent step for any organization.

In this case the commission’s findings did not inflict any financial damage on the organization. However, with these findings the former employee may choose to take further legal action against his employer that may lead to future financial damages in the future.

Inform all of your employees that they should not store personal passwords on company computers and inform all of your employees that they should not be eavesdropping on non-work related communications of other employees.

Source

Alberta Office of Information and Privacy Commission Order P2013-07