CLEARING THE CACHE: BC COURT ORDERS FOR RETURN OF DATA IN PRIVACY BREACH DISPUTE

Posted on July 8, 2024

Categories: Insights, Publications

In *British Columbia (Attorney General) v. Gondor*, 2024 BCSC 1077, the British Columbia Supreme Court considered the granting of a court order for the return and destruction of internal files leaked in a privacy breach dispute between a former employee and his employer who is a public body.

This decision provides an example of a remedy that a public body may seek in the event personal information in their custody or under their control was obtained by a person or an entity without authorization.

Background

Before the end of his employment, a Manager of Information Technology at the District of Saanich (the "**District**"), allegedly downloaded electronic records of the District (the "**Identified Records**") onto his work computer and a USB memory stick. The Identified Records contained personal information of the District's residents.

In March 2022, after the former employee had left his position with the District, the District learned from the Office of the Information and Privacy Commissioner for British Columbia that it had received two anonymous DVDs containing the District's records, including some of the Identified Records. On March 24, 2022, the former employee's son emailed the District complaining about his neighbour and attaching documents from the Identified Records.

Through technical investigations, the District was of the view the Identified Records were in the possession of the former employee and that he had no authorization to possess the information. The District then asked the Attorney General to petition the Court for an order requiring the return and destruction of the Identified Records pursuant to section 73.2 of the *Freedom of Information and Protection of Privacy Act* ("***FIPPA***").[1]

Legal Analysis

Requirements of section 73.2 of FIPPA

In assessing whether personal information should be returned under section 73.2, the following five-part test

must be met:[2]

1. The material in question must be personal information as defined in *FIPPA*;
2. The personal information must be in the custody or under the control of a public body;
3. The personal information must be in the possession of a person or entity not authorized by law to possess it;
4. There must have been a demand in writing for the return of the personal information or its destruction in the case of electronic records; and
5. The recipient of the demand must have failed to comply adequately.

The Court determined that only the third element of the test was seriously at issue, finding all other factors satisfied by the evidence provided and surrounding circumstances of the case.

Possession of Private Information by an Unauthorized Party

The Court found that the inconsistencies in the former employee's evidence in conjunction with the implausibility of his account of events were unpersuasive in absolving himself from suspicion. These incongruencies led the Court to conclude that the evidence established, on a balance of probabilities, that the former employee not only had acquired possession of the Identified Records without authorization, but had also disseminated copies of the Identified Records without authorization. The Court granted the Attorney General an order requiring the former employee to return or destroy the Identified Records and any copies in his possession. The order also required the former employee to disclose the names of anyone who was provided copies of the Identified Records.

Key Takeaways

This case highlights a method available to public bodies to recover personal information that had been acquired by individuals without authorization. The same remedy is not, however, available to private organizations under British Columbia's Personal Information Protection Act.[3] Private organizations may refer to McMillan's previous bulletin on best practices when faced with a privacy breach.

Given the significant business implications for organizations following a privacy breach, it is important to engage external counsel early in the process to obtain advice on applicable legal and regulatory requirements arising from a breach and to manage associated legal risks.

[1] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.
[2] The five-part test was drawn from *British Columbia (Attorney General) v Fuller*, 2018 BCSC 1981 at para 6.
[3] *Personal Information Protection Act*, SBC 2003, c 63.

by Yue Fei, Kristen Shaw, Claire Wanhella, and Brandon Hsu (Summer Law Student)

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.