Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 265-2018, 266-2018

Moose Jaw Police Service

January 7, 2020

Summary: The Moose Jaw Police Service (MJPS) proactively reported to the Office of the Information and Privacy Commissioner that two of its employees had intentionally accessed internal police information systems for their own personal use. MJPS investigated the breaches, and eventually terminated each employee because of their disregard for MJPS' privacy policies and training, as well as their oaths of secrecy. The Commissioner found that *The Local Freedom of Information and Protection of Privacy Act* was engaged, and was satisfied with how the MJPS investigated each breach and the sanctions it applied to each employee in response.

I BACKGROUND

[1] On November 6, 2018, the Moose Jaw Police Service (MJPS) proactively reported two separate privacy breaches ("Breach A" and "Breach B") to my office. The privacy breaches involved unauthorized system accesses or "snooping".

[2] On November 15, 2018, MJPS provided my office with summaries for Breaches A and B that included details related to each breach and the initial contents of its internal investigation. The details regarding each breach included the following:

Breach A

- On September 17, 2018, MJPS received a call from the parent of an alleged young offender with concerns that Employee A had shared the alleged young offender's police file information with a third party.

- Upon review of log information for Versaterm (the application MJPS uses to record information on investigations), MJPS determined Employee A had queried the young offender on September 1, 2018. A minute after Employee A logged off, their Internet history indicated that they had sent a message to a family member (the third party) through Facebook. MJPS determined the message included details from the alleged young offender file, excluding their name. When MJPS interviewed Employee A, they admitted they had accessed this information.

Breach B

- On October 2, 2018, Employee B, who was off-duty at the time, asked an on-duty communications officer to search license plate information in the system to find the owner of a vehicle that had allegedly been involved in an accident with Employee B's child. The on-duty communications officer refused, stating that it was not work-related. Employee B stated they would contact the communications officer who was on-duty later that day, who also happened to be Employee A.

[3] On November 26, 2018, my office asked MJPS to complete its formal investigation into Breaches A and B. MJPS provided additional information to my office on November 30, 2019. At the same time, MJPS noted it had terminated the employment of Employee A on November 22, 2018, and that of Employee B on November 22, 2018.

II DISCUSSION OF THE ISSUES

1. Does my office have jurisdiction?

[4] MJPS is a local authority pursuant to subsection 2(f)(viii.1) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Thus, I have jurisdiction to investigate this matter.

2. Did MJPS respond appropriately to the privacy breaches?

[5] If a privacy breach occurs, my office analyzes the steps taken by the local authority in managing the breach. These best-practice steps, which are outlined in my office's, *Privacy*

Breach Guidelines for Government Institutions and Local Authorities (May, 2018), include:

1. Contain the breach;
2. Notify affected individuals and/or appropriate organizations;
3. Investigate the breach;
4. Develop and implement a plan to prevent future breaches; and
5. Complete a report.

[6] I will analyze MJPS' management of these privacy breaches against these best practice steps.

Contain the Breach

[7] The first step is to contain the privacy breach, which means to prevent it from being ongoing. This includes taking actions such as recovering the information/records, stopping the unauthorized practice or access, shutting down the system that has been compromised or breached, revoking access privileges and correcting technical weaknesses in applications or software.

[8] With respect to Breaches A and B, MJPS took the following steps once it became aware of each breach:

Breach A

- On October 16, 2018, Employee A was suspended from duties and had their access to all MJPS systems/applications revoked pending an investigation by the MJPS.
- MJPS sent officers to interview the recipient, who resides in a different province, of the Facebook message that contained the alleged young offender's information); MJPS did not know, however, the details of the interview or if the recipient was advised not to delete the Facebook message or to not further disseminate the information.

Breach B

- On October 31, 2018, Employee B was suspended from duties and their access to all MJPS systems/applications was revoked pending investigation by the MJPS.

[9] I find that Breaches A and B were contained, and that MJPS took appropriate steps including sending police officers to talk to the recipient of the Facebook message in Breach A. I do note, however, that in Breach A, MJPS was not able to confirm if the recipient would have been told to delete the Facebook message or to not further disseminate the information.

[10] With respect to Breach A, I wish to commend MJPS for taking the additional steps to verify the extent to which the information had been disclosed by Employee A through Facebook. In Investigation Review Report 090-2017, my office reviewed the matter of a City of Saskatoon (the "City") bus driver who alleged the City violated their privacy by using surveillance footage to investigate a complaint against them. My office determined that a local authority has the right to collect and use employee information in such a manner in order to aid an investigation into the employee's actions. By checking into Employee A's Internet usage history within the same timeframe as when Employee A accessed Versaterm, the MJPS was able to determine how Employee A disclosed the information and to what extent.

Notify affected individuals and/or appropriate organizations

[11] Notifying an individual that their personal information was involved in a privacy breach is an important best practice step. This is so that affected individuals can take measures to protect themselves from potential harm resulting from the breach. It also acknowledges that individuals may feel hurt or humiliated by the type of personal information about them that was breached.

[12] A notification also provides a local authority the opportunity to apologize for the breach that has occurred, to reassure individuals that steps have been taken to prevent similar breaches from occurring in the future, and to make individuals aware of their right to raise concerns with my office.

[13] With respect to notification, MJPS undertook the following steps:

Breach A

- On September 21, 2018, MJPS contacted the young offender by phone to advise them that their personal information may have been breached. It followed up with them again by phone on October 5, 2018 and on November 22, 2018, to advise them of the outcome of the investigation and that Employee A had been terminated as a result of inappropriately accessing police systems for personal use.

Breach B

- With respect to Breach B, MJPS chose to not provide notification regarding the access to license plate information because Employee B did not appear to have used this information. Because of this breach, however, the MJPS audited Employee B's activities and discovered further breaches, which the MJPS investigated. As part of their investigation, MJPS provided notification to those affected individuals.

[14] Upon learning of the breaches, MJPS engaged its internal Privacy Officer in a timely manner, and provided notification of the breaches to my office once it had begun its internal investigation process. MJPS also confirmed with my office that it provided affected individuals with internal contact information in case there were questions, and that it also advised them of their right to raise concerns with my office.

[15] Based on the actions that MJPS took with respect to notification, I find that MJPS provided appropriate notification to the affected individuals.

[16] I do wish to add that MJPS further advised my office that it released a media statement at the time the employees were terminated. In the news release, MJPS stated, "The Moose Jaw Police Service recognizes its fundamental responsibility to protect the security of personal information it receives". While a media release is not a typical step a public body might take, I commend MJPS for taking this step in order to demonstrate to the public the value it places on protecting the public's personal, and also, very sensitive information.

Investigate the breach

[17] To investigate a privacy breach is to understand what happened that led to the breach. As part of this investigation, the local authority should determine the root cause, which will assist in managing the breach and implementing a plan to prevent similar breaches from occurring.

[18] As part of its investigation into Employee A, on or about October 3, 2018, MJPS audited the system and found that Employee A had accessed the system for the license plate information (for Employee B) and attributed the search to someone else. As I noted at paragraph [10], MJPS also undertook an audit of Employee A's Internet usage to determine the extent to which Employee A had disseminated information on the alleged young offender, and found that they had sent the information through Facebook, which is not a secure platform.

[19] When asked about their multiple accesses by the MJPS, Employee B admitted that they had made these accesses out of interest and curiosity. Employee B had no job-related reasons to access this information.

[20] Pursuant to subsection 23.1 of LA FOIP, local authorities have a duty to protect personal information in its possession or control, including having established policies and other safeguards regarding the protection of personal information. This ensures that employees are aware of their obligations under LA FOIP to protect personal information.

[21] With respect to policies, MJPS provided my office with a copy of its policy and procedures for the use of CPIC. The CPIC policy applies to all staff who have access to CPIC, which Employees A and B did. Upon review of the CPIC policy, I note that it states, "Under no circumstances will a printout or information about a criminal record be provided to a member of the general public". The policy also notes that when making an access to CPIC, employees are required to include a note regarding the reason for conducting the inquiry.

[22] MJPS confirmed with my office that Employee A took its in-house privacy training on November 6, 2017, while Employee B took theirs on October 30, 2018. Employees A and

B also signed an "Oath of Secrecy" upon commencement of employment, which states explicitly that, "I will not allow any person or persons to inspect or have access to any written statement, Police Service record…" Employee B had also been warned by a co-worker that accessing the system for personal use was a violation of LA FOIP, and that the co-worker did not want to participate in the snooping because they did not want to lose their own job.

[23] It seems that Employees A and B each should have had knowledge of their roles with respect to LA FOIP and their obligations to protect personal information. The actions each employee took directly contravened MJPS policy, what they were taught in training, and their "Oath of Secrecy". I find that MJPS appropriately investigated Breaches A and B and that the root cause was that Employees A and B disregarded MJPS policy, their privacy training, and their "Oath of Secrecy".

Develop and implement a plan to prevent future breaches

[24] While a local authority cannot undo a privacy breach, it can learn from and improve its practices by formulating a prevention plan. As noted in my office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, one of the most important aspects of ensuring the prevention of future breaches is to ensure appropriate safeguards exist.

[25] As noted previously in this Report, MJPS terminated Employees A and B. This is an appropriate step to take to prevent a similar privacy breach from occurring.

[26] With respect to creating further safeguards, privacy training is another way to help prevent privacy breaches from occurring. Upon review of MJPS' training curriculum, I am impressed with the variety of topics covered in the training for those employed by MJPS:

- General overview of federal and provincial privacy laws, including responsibilities and obligations of the police and staff under LA FOIP;
- Roles and responsibilities of the privacy coordinator, IT individuals and staff;

- Key privacy concepts, including collection, use and disclosure pursuant to LA FOIP, as well as need-to-know;
- Strategies for managing and protecting information, including retention;
- Access provisions, including exemptions; and
- Developing an access and privacy program, including the role of the Information and Privacy Commissioner.

[27] Another important safeguard is proactive auditing. MJPS advised my office that some of the outside applications and databases it accesses are routinely audited by their hosting organizations. With respect to its own system, Versaterm, MJPS advised that currently it conducts system audits if it is suspected there has been an unauthorized access. In my Review Report 260-2017 at paragraph [33], I discussed the importance of proactive auditing to assess compliance with and measure effectiveness of policies and procedures. This type of auditing does not need to be exhaustive; it can include, for example, auditing on random samples at specific time intervals, the development of specific flags such as same-name or user/organization lookup, lookups without user notes, lookups on high-profile cases, or look ups on cases that are resolved or completed. While the MJPS does perform auditing on Versaterm, I recommend that it strengthen this by implementing proactive audits.

[28] I find that MJPS is taking appropriate steps to prevent similar privacy breaches from occurring in the future, but do recommend that it implement proactive audits.

Complete a report

[29] By documenting its investigation into a privacy breach, a local authority sets a method to ensure it continues to follow through with plans to prevent similar breaches in the future.

[30] I find that the MJPS has completed its investigation report and that it contained all the necessary elements.

[31] I must note that the MJPS has only been under LA FOIP for a relatively short period of time, but it nonetheless has developed a comprehensive approach to the protection of

privacy and is treating privacy breaches seriously. I applaud MJPS for its efforts and how it has managed these privacy breaches.

III FINDINGS

[32] I find that Breaches A and B were contained.

[33] I find that MJPS provided appropriate notification.

[34] I find that MJPS appropriately investigated Breaches A and B and that the root cause was that Employees A and B disregarded MJPS policy, their privacy training, and their "Oath of Secrecy".

[35] I find that MJPS is taking appropriate steps to prevent similar privacy breaches from occurring in the future.

IV RECOMMENDATION

[36] I recommend that the MJPS implement proactive audits for Versaterm.

Dated at Regina, in the Province of Saskatchewan, this 7th day of January, 2020.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner