Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 228-2015

Saskatchewan Power Corporation

June 22, 2016

Summary: The SaskPower Corporation (SaskPower) proactively reported a case of employee snooping to my office. SaskPower advised that an employee had inappropriately accessed personal information of 4,382 current and former SaskPower employees and copied two files from that data. The Commissioner recommended that SaskPower amend its Code of Conduct to specifically address employee snooping and incorporate it into employee training. The Commissioner also recommended SaskPower contact the Association of Professional Engineers and Geoscientists to report the former employee, if he is a member. Finally, the Commissioner recommended that SaskPower forward its investigation file to the Ministry of Justice, Public Prosecutions Division.

I BACKGROUND

[1] On December 18, 2015, Saskatchewan Power Corporation (SaskPower) contacted my office to proactively report a case of employee snooping. SaskPower indicated that it believed the privacy breach involved the inappropriate access of more than 1000 employee human resource files, potentially over the span of several years. On December 22, 2015, SaskPower notified my office that there were approximately 4800 current and former employees affected by this breach of privacy.

[2] On December 22, 2015, my office provided notification to SaskPower advising that my office would be monitoring the matter and requested that SaskPower provide a copy of its internal privacy breach investigation report once completed.

[3] SaskPower concluded that this breach of privacy resulted from the employee extensively searching network drives, and both previewing and saving files to his corporate workstation without a legitimate business purpose. He copied two files from the data searches that contained the personal information of current and former SaskPower employees:

1. A Microsoft Office database, copied on March 17, 2015, containing records for 3,135 current and former employees that included name, employee number, social insurance number, sex, marital status, home mailing address, home phone number, salary, spouse name and gender, life insurance coverage and beneficiaries; and

2. An Excel file, copied on April 9, 2013, containing records for 2,402 current and former employees including name, employee number, social insurance number, birthday, start date, department and position.

[4] As some employees were on both lists, SaskPower determined that the total number of affected current and former employees was 4,382.

[5] Upon conclusion of SaskPower's investigation, the employee's employment with SaskPower was terminated on January 8, 2016.

II DISCUSSION OF THE ISSUES

[6] SaskPower is a "government institution" pursuant to subsection 2(1)(d)(ii) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

1. Did SaskPower follow best practices in its response to these privacy breaches?

[7] In circumstances where there is no dispute that a privacy breach has occurred, the focus for my office becomes one of determining whether the public body has appropriately handled the privacy breach. In order to be satisfied, my office would need to be confident that SaskPower took the privacy breach seriously and appropriately addressed it. My office's resource, *Privacy Breach Guidelines* recommends four best practice steps to be taken by public bodies when responding to privacy breaches. These are:

1. Contain the breach
2. Notify affected individuals and/or appropriate organizations
3. Investigate the breach
4. Prevent future breaches

[8] I will weigh the appropriateness of SaskPower's handling of this privacy breach against these four best practice steps.

i. Contain the Breach

[9] Upon learning that a privacy breach has occurred, public bodies should immediately take steps to contain the breach. Depending on the nature of the breach, this can include:

- Stopping the unauthorized practice;
- Recovering the records;
- Shutting down the system that has been breached;
- Revoking access privileges; or
- Correcting weaknesses in physical or electronic security.

[10] According to SaskPower's internal investigation and forensic analysis reports, they took a number of measures to identify and contain the breach:

1. SaskPower's Enterprise Security team initiated a SaskPower network scan while investigating a non-privacy related incident at SaskPower around November 9, 2015. As a result of that scan, a large caché of files on the employees' workstation was discovered. Enterprise Security began monitoring the employees' workstation and revealed that the employee routinely performed searches against network drives for files that were modified or created during recent date ranges.

2. The Director of Internal Audit and Manager, Security Investigations, Enterprise Security interviewed the employee on November 19, 2015. During this interview, the employee denied sending any documents outside of SaskPower Corporation. The employee also volunteered his personal Blackberry and several removable USB drives and two external hard drives for analysis. The employee then contacted the Director of Internal Audit regarding an additional USB in his home. The Director and Manager met the employee at his curbside to retrieve the USB.

3. On November 19, 2015, the employee was suspended with pay pending an investigation.

4. During the analysis of the media retrieved from the employee, SaskPower identified that the employee copied the following two files onto the removable media:

    i. On a USB drive a Microsoft Access database containing records for 3,135 current and former employees including their name, employee number, social insurance number, sex, marital status, home mailing address, home phone number, salary, spouse name, spouse gender, life insurance coverage, family insurance coverage type and beneficiaries; and

    ii. On a portable hard drive an excel file containing records for 2,402 current and former employees including their name, employee number, social insurance number, bargaining unit, birthday, start date, department and position.

5. SaskPower scanned the network to determine if any additional copies were on other workstations or network drives. This scan resulted in no additional copies being located.

[11] SaskPower's internal investigation report indicated that no evidence was found to show that the employee distributed or forwarded the personally identifiable information to any other persons from his workstation.

[12] SaskPower was unable to trace if the information was shared once it was at the employee's residence on the unencrypted removable storage devices. However, SaskPower advised my office that the employee denied sharing any information outside of SaskPower when he was interviewed by both the RCMP and SaskPower. Further, SaskPower advised it had not received any complaints of fraudulent activity or problems with what was breached from the affected individuals as of the date of this report.

[13] I find that SaskPower has taken every reasonable step to contain the breach of privacy.

ii. Notify affected individuals and/or appropriate organizations

[14] Notifying an individual that their personal information has been inappropriately accessed is important for a number of reasons. Not only do individuals have a right to know, they need to know in order to protect themselves from any potential hardship that may result

from the inappropriate access. Unless there is a compelling reason not to, public bodies should always notify affected individuals.

[15] In addition to notifying individuals, public bodies may want to notify other organizations, for example, my office, law enforcement or other regulatory bodies that oversee particular professions.

[16] In this case, SaskPower verbally notified my office of the privacy breaches on December 18, 2015. SaskPower provided notification to the 4,382 affected individuals by letter dated December 21, 2015. The notification included:

1. A general description of the compromised data elements.
2. The contact information of the SaskPower's Chief Privacy Officer so the affected individuals could learn more about what specific information was breached.
3. Contact information for my office.
4. An apology.

[17] On December 22, 2015, SaskPower posted information about this breach of privacy on SaskPower's Employee Information Network. On December 28, 2015, information was communicated to managers and supervisors in a weekly communication memo.

[18] My office began receiving telephone calls from affected individuals on December 23, 2015. In the majority of these calls, the individuals were asking what information had been breached and if they should be concerned. Information and Privacy Commissioner (IPC) staff referred callers back to SaskPower as our office did not have details regarding which pieces of personal information were involved for each individual. The affected individuals would advise that they have either already left a message or the voice mailbox was full and they were unable to leave a message.

[19] Through conversations with SaskPower, we were advised that the Chief Privacy Officer had received hundreds of telephone calls. In addition, he had experienced technical issues with retrieving voicemails from his message manager, requiring an alternate method of accessing them.

[20] With the number of affected individuals in this breach, the amount of potential inquiries was much more than one official could handle. Had SaskPower established a strategy for handling these calls in advance of sending notification, the affected individuals would have been able to have their questions and concerns addressed more quickly. However, it does appear that SaskPower remedied this situation. In addition, SaskPower has advised my office they are looking at solutions to handle inquiries should a future breach occur.

[21] SaskPower is also initiating further communications regarding this breach. This includes communicating through SaskPower's internal employee intranet for all current employees and through a newsletter that is sent to former SaskPower employees, including retirees. These communications will reiterate what employees were advised in the original notification letter, including steps to take if they have concerns. I would suggest SaskPower ensure that all affected individuals would have access to one of these communications, and if not send those individuals without access, a follow-up notification letter.

[22] In addition to notifying the affected individuals and my office, SaskPower referred this to the municipal police on December 7, 2015. It was referred to the RCMP on December 10, 2015 due to the geographic location of the employee's workplace. SaskPower was notified that the RCMP interviewed the employee on January 8, 2016. In that interview he denied sharing the information outside of SaskPower.

[23] SaskPower advised my office that the RCMP referred the case to the Crown Prosecutor's Office.

[24] SaskPower has advised my office that as of the date of this report they have not received any complaints of fraudulent activity from the affected individuals, and SaskPower continues to monitor this situation.

[25] The employee may be a member of the Association of Professional Engineers and Geoscientists of Saskatchewan (APEGS). From its website, APEGS regulates the practice of engineering and geoscience in Saskatchewan. Part of this role is to investigate

complaints about its members and hold discipline hearings. SaskPower advised my office they have not contacted APEGS to determine if he is a member. Therefore, SaskPower should contact APEGS to determine if he is a member and if so, report the former employee to APEGS.

[26] Except for SaskPower not contacting APEGS, I am satisfied that SaskPower sufficiently provided notice of this privacy breach.

iii. Investigate the Breach

[27] Once the breach has been contained and the appropriate notification has occurred, the public body should conduct an internal investigation. The investigation is generally conducted by the public body's Privacy Officer because they have the appropriate privacy expertise to do so and understand what the relevant privacy legislation requires of their organization. The investigation should be documented in an internal privacy breach investigation report and include a root cause analysis. At the conclusion of its investigation, the public body should have a solid grasp of what occurred.

[28] On January 6, 2016, SaskPower provided my office with its investigation materials which included a seven page investigation report conducted by Internal Audit and a 32 page forensic analysis report conducted by SaskPower's Enterprise Security team.

[29] During SaskPower's investigation, the investigators determined the employee had more access to the network drives than was required to perform his work duties. SaskPower had assumed they had the appropriate safeguards in place to restrict access to network drives to those with a legitimate business need-to-know but that was not the case. Because of this, the employee was able to inappropriately access and copy files that contained the personal information of current and former employees.

[30] SaskPower requires all employees take privacy training on an annual basis. The employee had completed his initial privacy awareness training on December 16, 2003 and his last recorded annual refresher was completed on May 14, 2013. In addition,

SaskPower has online employee Code of Conduct training that includes a privacy and confidentiality component and SaskPower requires that all employees take this training on an annual basis. The employee completed this initial training October 1, 2013 and the annual refresher on February 11, 2015.

[31] SaskPower has provided my office with sufficient detail to show that this matter was investigated adequately.

[32] Due to the number of records the employee snooped into, if SaskPower has not sent its final report to the Ministry of Justice, it should forward its investigation file including the internal investigation and forensic analysis report to the Ministry of Justice, Public Prosecutions Division. This would allow prosecutors to further consider whether an offence has been committed and if charges should be laid under FOIP or any other statute.

iv. Prevent Future Breaches

[33] The final step is to formulate a plan to avoid future breaches of a similar nature. Some changes that are needed may have revealed themselves to the public body during the investigation phase such as deficient policies or procedures, a weakness in the system, a lack of accountability measures or lack of training. This is an important step in addressing a privacy breach because a privacy breach cannot be undone but the public body can learn from it and improve.

[34] As SaskPower determined this privacy breach was able to occur as network drives were not sufficiently restricted, a number of systems security improvements were initiated. Some of these steps included:

1. Lock the affected network folders and verify with the business areas to ensure only authorized units would have access.

2. Verify security controls on network folders containing confidential information.

3. Procure an additional reporting tool that will enable large-scale audit assessments on systems that contain private, confidential and restricted information. The initial audits are focusing on those areas containing the information deemed as the most high-risk.

4. Continue to monitor SaskPower systems to ensure there are no further instances of the two files containing the employee information.

[35] SaskPower advised my office that they did not have a policy in place that specifically addressed the issue of employees bringing removable storage devices from home, or taking removable storage devices from SaskPower property. SaskPower indicated that they are in a process of drafting a policy to address this issue.

[36] SaskPower has initiated a tracking process through Human Resources to ensure that all employees complete mandatory privacy training on an annual basis. Employees will be reminded of this each January during performance discussions. SaskPower's Vice Presidents and Directors will receive semi-annual updates of which employees have not taken the annual mandatory training to ensure completion each year.

[37] SaskPower provided my office with the Code of Conduct that, in part, speaks to employees' protection of privacy obligations but does not speak specifically to the issue of employee snooping. Therefore, SaskPower should revise the Code of Conduct to specifically address employee snooping and incorporate this into initial and annual training.

[38] Provided SaskPower amends its employee Code of Conduct and training to address employee snooping, I am satisfied with the steps SaskPower has taken to prevent future occurrences of employee snooping incidences.

III FINDING

[39] I find that SaskPower has adequately responded to the privacy breach and implemented sufficient safeguards to prevent future occurrences.

IV RECOMMENDATIONS

[40] I recommend SaskPower amend its Code of Conduct to specifically address employee snooping and incorporate employee snooping into initial and annual training.

[41] I recommend SaskPower contact APEGS to inquire if the former employee is a member and if he is, report him to APEGS.

[42] If it has not done so, I recommend SaskPower forward its investigation file including the internal investigation and forensic analysis report to the Ministry of Justice, Public Prosecutions Division. This would allow prosecutors to further consider whether an offence has occurred and if charges should be laid under FOIP or any other statute.

Dated at Regina, in the Province of Saskatchewan, this 22nd day of June, 2016.

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