Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 111-2017

Ministry of Labour Relations and Workplace Safety

September 28, 2017

Summary: Privacy breaches occurred when employees of the Ministry of Labour Relations and Workplace Safety (LRWS) attempted to print documents containing personal information to printers within their offices but were actually being printed at the printer located at the Saskatoon Correctional Centre. The Information and Privacy Commissioner (IPC) made a number of recommendations including that the Ministry of Central Services (Central Services) establish written policies and/or procedures on how it will use a IT script it has developed to remove users from printers when printers are removed from a workplace and how it will inform users to remove printers from their desktops and applications at the time printers are removed from the printer.

I BACKGROUND

[1] In October 2016, the Ministry of Labour Relations and Workplace Safety (LRWS) proactively reported a privacy breach to my office. An employee at its office in North Battleford had intended to print a document containing personal information from an Oracle application to a printer within the office. The print job was not only sent to a printer within its North Battleford office, it was also sent to a printer located at the Saskatoon Correctional Centre. This resulted in a privacy breach (incident #1).

[2] Through its investigation, LRWS (with Information Technology Division (ITD) at the Ministry of Central Services) determined that the Oracle application was set to send print jobs to the printer at the Saskatoon Correctional Centre. While neither LRWS nor ITD could explain at that time why this had occurred, they both took steps to prevent a similar breach. To ensure a similar breach would not occur, the employee printed a document

from the Oracle application to make sure that print jobs were no longer being sent to the Saskatoon Correctional Centre. Saskatoon Correctional Centre confirmed that its printer did not print the document.

[3] LRWS provided my office with additional information on how it managed the privacy breach, including how it contained the breach, notified the affected individual of the breach, investigated the breach, and took steps to minimize the likelihood of a similar incident from occurring. Since LRWS took reasonable steps to manage the privacy breach, my office had determined that the above matter was informally resolved.

[4] However, on June 1, 2017, LRWS proactively reported another privacy breach to my office (incident #2). This privacy breach is very similar to Incident #1. An employee attempted multiple times to send a print job to a printer located at LRWS' Saskatoon office. Eventually, he was successful. However, in the course of attempting to print the email, the email printed twice by the same printer involved in Incident #1 at the Saskatoon Correctional Centre.

[5] My office notified LRWS that it would be undertaking an investigation. Further, it contacted the Ministry of Central Services (Central Services) to provide information for the purpose of my office's investigation.

[6] One of the purposes that I hope to achieve through this Investigation Report is to raise awareness among Government of Saskatchewan employees regarding this issue. Similar incidents may be occurring across government institutions. Through this investigation, my office has determined that awareness and education among employees across government will be helpful in preventing similar privacy breaches. As detailed later in this report, Central Services indicated to my office it will take steps to prevent similar breaches. However, it also needs to rely on employees to proactively remove printers from their workstations and applications when printers are decommissioned.

II DISCUSSION OF THE ISSUES

[7] LRWS is a government institution pursuant to subsection 2(1)(d)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP).

1. Did a privacy breach occur?

[8] A privacy breach occurs when personal information is collected, used, and/or disclosed in a way that is not authorized by FOIP.

[9] Subsection 24(1) of FOIP defines "personal information" as follows:

> Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:

[10] A disclosure occurs when personal information is shared with an entity separate from the government institution. Government institutions must only disclose personal information pursuant to subsection 29(1) of FOIP, which provides:

> 29(1) No government institution shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 30.

[11] In both incidents #1 and #2, personal information was disclosed to the Saskatoon Correctional Centre. Such a disclosure was not authorized by subsection 29(1) of FOIP. Therefore, I find a privacy breach occurred in both incidents.

2. Did LRWS respond to the privacy breach in incident #2 appropriately?

[12] As noted in the background section of this report, my office had found that LRWS had responded to incident #1 appropriately. Therefore, this report will focus on whether LRWS responded to incident #2 appropriately.

[13] My office suggests that government institutions undertake the following five steps when responding to a privacy breach:

- Contain the breach
- Notify affected individual(s)
- Investigate the privacy breach
- Prevent future privacy breaches
- Write an investigation report

[14] My office will analyze each step below.

Contain the breach

[15] To contain the breach is to ensure the personal information is no longer at risk. This may include recovering the records, revoking access to personal information, and/or stopping the unauthorized practice.

[16] According to its privacy breach report, Saskatoon Correctional Centre had sealed the two physical copies of the email in an envelope and returned them to LRWS. Therefore, I find that the breach has been contained.

Notify affected individual(s)

[17] Notifying affected individuals of the privacy breach as soon as possible is important so individuals can determine how they have been impacted and they can take steps to protect themselves. Notification should include the following:

- A description of what happened,
- A detailed description of the personal information that was involved,
- A description of possible types of harm that may come to them as a result of the privacy breach,
- Steps that the individuals can take to mitigate harm,
- Steps the trustee is taking to prevent similar privacy breaches in the future,
- The contact information of an individual within the government institution who can answer questions and provide further information,
- A notice that individuals have a right to complain to the Office of the Information and Privacy Commissioner (OIPC),

- Recognition of the impacts of the breach on affected individuals and an apology.

[18] According to its privacy breach report, LRWS did not notify the affected individual. Its reason is because the breach was confined and secured by a government employee.

[19] There should be compelling reasons not to notify affected individuals. In this case, there is no compelling reason not to notify the affected individual. In the course of this investigation, my office recommended that LRWS notify the affected individual. LRWS indicated to my office that it will notify the affected individual.

Investigate the privacy breach

[20] Investigating the privacy breach to identify the root cause is key to understanding what happened and to prevent similar breaches in the future.

[21] In its privacy breach report, LRWS was able to determine that the printer at Saskatoon Correctional Centre was a printer used by LRWS in the past. It was decommissioned and then redeployed to the Saskatoon Correctional Centre.

[22] Since Central Services provides Information and Technology (IT) services for the Government of Saskatchewan, my office contacted Central Services for information about both Incident #1 and Incident #2, and its processes related to installing and removing printers, as well as decommissioning and redeploying printers.

[23] Central Services indicated that employees install printers on their own workstations. That is, employees are able to select which printer best suits them to print. However there is no ability for it to centrally remove users when printers are decommissioned. An oversight likely occurred when employees were not instructed to remove the printer when the printer was decommissioned from LRWS and redeployed to the Saskatoon Correctional Centre.

Prevent future breaches

[24] Preventing future breaches means to implement measures to prevent future breaches from occurring.

[25] After incident #2 occurred, LRWS had its employees in Saskatoon review which printers were installed to their workstations. Four employees had the printer installed to their workstation. These employees removed the printer from their workstations.

[26] In efforts to prevent a similar privacy breach, Central Services indicated to my office that it developed an IT program/script that removed LRWS employees from being able to print to the Saskatoon Correctional Centre. It said this script will be used across government to remove users from printers when printers are removed from the workplace. However, the script will only remove current users whose computer is powered on at the time the script is executed. Furthermore, a user would still have the ability to add the printer back to their workstation after the script has removed it.

[27] Central Services also indicated that it will inform users of the requirement to remove printers from their desktops and applications at the time printers are removed from the workplace.

[28] I find that the above steps that have been (and will be) taken by Central Services to be reasonable to prevent future privacy breaches. If it has not already done so, I recommend that Central Services establish a written policy and/or procedure so that the IT script will be used to remove users from printers when printers are removed from a workplace and that it will inform users of the requirements to remove printers from their desktops and applications at the time printers are removed from the workplace.

[29] In addition to the above efforts by Central Services to prevent a future privacy breach, it said it relies on employees to proactively remove printers when the printer is removed. I recommend that Central Services create awareness materials, such as guidelines, brochures, or posters, that informs users on how to remove printers (or other devices) when they are decommissioned. Such materials can also include Central Services' contact information so users can contact Central Services for assistance.

[30] Finally, in the course of this investigation, my office recommended that Central Services work together with ministries so that the default settings on workstations and mobile devices from which employees print documents are set to print securely, especially where there are a large number of employees printing to a common printer or where documents containing personal information are printed regularly to a common printer. That is, printers will store print jobs and they will print documents when the user is physically at the printer and enters a passcode. Central Services indicated to my office that it does not have the technology in place to control the default settings of users. However, it will develop a communication piece related to secure print. Users will be encouraged to use the secure print option as their default printer setting and instructions will be provided on how to change their default settings to the secure print option.

Write an investigation report

[31] Documenting the privacy breach and the government institutions investigation into the matter is a method to ensure that the government institution follows through with plans to prevent similar privacy breaches in the future.

[32] LRWS provided my office with its privacy breach report, which has been referenced throughout this report. I find that LRWS has documented this privacy breach and its investigation well.

III FINDINGS

[33] I find a privacy breach occurred in both Incident #1 and Incident #2.

[34] I find that LRWS contained the breach.

[35] I find that LRWS did not notify the affected individual.

[36] I find that the steps that have been (and will be) taken by Central Services to be reasonable to prevent future privacy breaches.

[37] I find that LRWS has documented this privacy breach and its investigation well.

IV RECOMMENDATIONS

[38] I recommend that LRWS follow through with notifying the affected individual in Incident #2 as described at paragraph [19].

[39] I recommend that Central Services, if it has not already done so, establish a written policy and/or procedure so that the IT script will be used to remove users from printers when printers are removed from a workplace and that it will inform users of the requirements to remove printers from their desktops and applications at the time printers are removed from the workplace.

[40] I recommend that Central Services create awareness materials, such as guidelines, brochures, or posters, that informs users on how to remove printers (or other devices) when they are decommissioned.

[41] I recommend that Central Services follow through with developing a communication piece related to secure print as described at paragraph [30].

Dated at Regina, in the Province of Saskatchewan, this 28th day of September, 2017.

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