Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 080-2020, 120-2020

Estevan Police Service

February 3, 2022

Summary: The Estevan Police Service (EPS) and the Complainant advised my office of a breach of privacy when EPS disclosed information to a lawyer containing the personal information of the Complainant. The Commissioner found EPS did not contain the privacy breach. In addition, the Commissioner found EPS provided appropriate notification of this breach of privacy. The Commissioner also found EPS conducted an adequate investigation of this matter. The Commissioner found EPS failed to meet its duty to protect the Complainant's personal information when it provided an unredacted copy of the record to the lawyer. Finally, the Commissioner found EPS has begun to take steps to mitigate the risk of this type of breach happening in the future. The Commissioner recommended EPS request again the law firm to apply to court to remove the exhibit and not cooperate with this law firm until the law firm makes the application to court to remove the exhibit. The Commissioner also recommended that EPS complete its policies and procedures regarding the disclosure of personal information that aligns with the requirements of section 28 of LA FOIP within the next three months. Finally, the Commissioner recommended EPS require privacy training for its employees on an annual basis.

I BACKGROUND

[1] On March 30, 2020, the Estevan Police Service (EPS) advised my office, in part, of the following:

> On March 9, 2020, a FOIP request was received from an applicant requesting any past and present reports made on [applicant], including on March 8, 2020.
>
> …
> On March 20, 2020, [FOIP Co-ordinator] reviewed the file, applied redactions, printed the file, prepared a partial access letter, and emailed the file and letter to the applicant.

> On March 24, 2020, [FOIP Co-ordinator] received a request from a lawyer requesting an unredacted police report from March 8, 2020, regarding his client [the applicant]. The lawyer was requesting the information to his office by Thursday, March 26, 2020, as they may file these materials with the Court this Friday, March 27, 2020.
>
> … As this file was no longer under investigation, and the request came from a lawyer, [FOIP Co-ordinator] thought [FOIP Co-ordinator] could provide them with the information.
>
> On March 27, 2020 … the [Complainant] who was affected by the privacy breach called EPS very upset, stating that [the Complainant's] personal information and a report from March 8, 2020, were released to the applicant and [Applicant's] lawyer.

[2] On April 4, 2020, my office notified EPS that my office would be opening an investigation on this matter and requested a copy of EPS' internal investigation report, any further details of the breach of privacy and copies of relevant documents.

[3] On May 5, 2020, the Complainant contacted my office to file a privacy complaint. On May 12, 2020, my office notified the Complainant that we would be investigating the matter.

II DISCUSSION OF THE ISSUES

1. Is *The Local Authority Freedom of Information and Protection of Privacy* Act engaged and do I have jurisdiction to investigate this matter?

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

[5] In a breach of privacy investigation, in order for LA FOIP to be engaged, there must be personal information involved as provided for in section 23(1) of LA FOIP. To qualify as personal information, the information must relate to an identifiable individual and be personal in nature.

[6] EPS provided me a copy of the information that was provided to the lawyer, Stephen Schuck. From a review of this information, the Complainant's information included:

- Name
- Date of birth
- Sex
- Address
- Phone number
- Summary of the Complainant's investigation request to EPS
- Details of the Complainant's contacts with EPS regarding the investigation
- Copies of correspondence sent by the Complainant to EPS and other organizations

[7] This type of information qualifies as personal information pursuant to sections 23(1)(a), (e), (f), (h), (k)(i) and (ii) of LA FOIP, which provides:

> **23**(1) Subject to subsections (1.1) and (2), "personal information" means personal information about an identifiable individual that is recorded in any form, and includes:
>
> (a) information that relates to the race, creed, religion, colour, sex, sexual orientation, family status or marital status, disability, age, nationality, ancestry or place of origin of the individual;
>
> ..
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;
>
> (f) the personal opinions or views of the individual except where they are about another individual;
>
> …
> (h) the views or opinions of another individual with respect to the individual;
>
> …
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
>
> (ii) the disclosure of the name itself would reveal personal information about the individual.

[8] Therefore, as there is personal information involved in this matter, LA FOIP is engaged.

2. Did a privacy breach occur?

[9] Section 28(1) of LA FOIP requires a local authority to have the consent of an individual in order to disclose their personal information unless authority to disclose without consent exists under sections 28(2) or 29 of LA FOIP. Section 28(1) of LA FOIP provides:

> **28**(1) No local authority 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 29.

[10] There is no need to consider whether EPS had authority to disclose the Complainant's personal information as EPS has already acknowledged the breach of privacy and proactively reported the breach to my office on March 30, 2020.

[11] As there is no dispute on whether there was a breach of the Complainant's privacy, I will move on to assessing whether EPS appropriately handled the breach according to my office's best practices.

3. Did EPS respond appropriately to the breach?

[12] In my office's resource, *Privacy Breach Guidelines for Government Institutions and Local Authorities*, updated September 2021 (*Privacy Breach Guidelines*), I recommend four best practice steps in responding to a privacy breach:

- Contain the breach
- Notification
- Investigate the breach
- Prevent future breaches

(*Privacy Breach Guidelines,* pp. 4-7)

[13] I will now consider if EPS responded to this matter appropriately against these four best practice steps.

Contain the Breach

[14] An important first step in responding to a privacy breach is to work to contain the breach immediately. In other words, ensure the personal information is no longer at risk. This may involve some or all of the following steps:

- Stopping the unauthorized practice
- Recovering the records
- Shutting down the system that was breached
- Revoking access to personal information
- Correcting weaknesses in physical security

(*Privacy Breach Guidelines*, p. 4)

[15] EPS advised my office:

> On March 30, 2020 … [EPS FOIP Co-ordinator] contacted the [lawyer] at 1100hrs and asked to have the electronic file deleted from [the lawyer's] email and server and to shred any copies that they may have. [EPS FOIP Co-ordinator] received an email back from [lawyer] at 1116hrs that all information was deleted from their server, and they didn't have any physical copies of the report except what was sworn and filed with the Courthouse in Regina.
>
> …
> At 1205 [EPS FOIP Co-ordinator] called the Queen's Bench Court and spoke with the Registrar/Executive Legal Officer asking how to go about getting an exhibit returned that was sworn and entered into evidence. [EPS FOIP Co-ordinator] was advised that all family files are sealed. As per section 15-4(1) of the Queen's Bench Rules – which states, No person other than a party, a party's lawyer or a person authorized by a party or by a party's lawyer may have access to (a) the Court record, including documents, exhibits, and section 15-5 - Any person who has access to documents obtained pursuant to the financial disclosure provisions of this Part or to evidence obtained pursuant to discovery or the Court record: (a) shall keep the documents and evidence, and any information obtained from them or from the Court record, in confidence.
>
> …
> April 2, at 0805hrs, [FOIP Co-ordinator] spoke with [Court of Queen's Bench] in Regina, and they advised that [the lawyer] that submitted the documents should complete the application to have the records removed and returned. [FOIP Co-ordinator] sent an email to [the lawyer] advising [the lawyer] of such and to let [EPS FOIP Co-ordinator] know once this was complete. [EPS FOIP Co-ordinator] called the [Complainant] at 0813 to inform [the Complainant] of such and had to leave a message to call me back.

[16] On April 29, 2020, the lawyer, Stephen Schuck emailed the following, in part, to EPS FOIP Co-ordinator:

> I spoke with [Registrar/Executive Legal Officer] at the Court of Queen's Bench in Regina this morning. I believe there was a miscommunication between the two of you as far as any obligation on my part to apply to Court in order to remove the material from the Court file.
>
> I wanted to reiterate that all materials filed in a family law matter are confidential. This means that report that was filed with the Court will not be shared with any third parties and the only parties who will review that material are those parties involved in the proceeding.
>
> With that said, any party seeking to have the material removed from the Court file is free to apply to Court and argue that it should be removed.
>
> If there is legislation that I am unaware of that compels me to apply to Court to remove this material; please have your legal counsel forward me a letter citing the legislation and particular section requiring me to do so. Beyond that, **I will not be bringing an application to have the materials removed from the Court file unless there is some legal basis provided obligating me to**.
>
> As mentioned before, there is nothing stopping the other party in a Court proceeding from bringing an application to have an exhibit removed from the file if they wish to do so.
>
> [Emphasis added]

[17] I am disappointed with the response of the lawyer. The lawyer may not have had a legal obligation to request removal of the exhibit. But it was the lawyer that asked for EPS' cooperation in providing the report. The lawyer also asked that it be provided right away. EPS attempted to cooperate. If not a legal obligation, the lawyer needs to think about the loss of cooperation in the future. I would recommend EPS request again the law firm to apply to court to remove the exhibit and not cooperate with this law firm until the law firm makes the application to court to remove the exhibit. That is the least this law firm can do in return for EPS facilitating their request on short notice.

[18] When EPS provided the unredacted copy of the record to the lawyer, it lost control of what would happen to the record once it was out of the control of EPS. As a result, I find EPS did not contain this breach of privacy.

Notification

[19] Once a privacy breach is discovered, the following is a list of individuals or organizations that may need to be notified as soon as possible after learning of the incident:

- Your organization's privacy officer
- My office
- The police, if criminal activity is suspected
- The affected individual(s) – unless there are compelling reasons why this should not occur

(*Privacy Breach Guidelines,* p. 4)

[20] It is important to note that LA FOIP requires that, if there is an unauthorized use or disclosure of personal information, the local authority must notify the affected individual if the "incident creates a real risk of significant harm" to the affected individual (see section 28.1 of LA FOIP). A real risk of significant harm is where there is some risk of damage, detriment, or injury to the individual that is significant in nature (*Privacy Breach Guidelines,* p. 4*)*.

[21] It is best to contact affected individuals directly, such as by telephone, letter, or in person. However, there may be circumstances where it is not possible, and an indirect method is necessary or more practical. Such situations would include where contact information is unknown or where there are a large number of affected individuals. An indirect method of notification could include a notice on a website, posted notices, media advisories, and advertisements. It is important to ensure the breach is not compounded when using indirect notification (*Privacy Breach Guidelines,* p. 5).

[22] Notifications should include the following:

- A description of the breach.
- A detailed description of the personal information involved.
- A description of possible types of harm that may come to them as a result of the privacy breach.
- Steps taken and planned to mitigate the harm and to prevent future breaches.

- If necessary, advice on actions the individual can take to further mitigate the risk of harm and protect themselves (e.g. how to contact credit reporting agencies, how to change a health services number or driver's license number etc.).
- Contact information of an individual within your organization who can answer questions and provide further information.
- A notice that individuals have a right to complain to the IPC (provide contact information).
- Recognition of the impacts of the breach on affected individuals and, an apology.

(*Privacy Breach Guidelines*, pp. 5-6)

[23] As noted above, EPS proactively reported this privacy breach to my office on March 30, 2020.

[24] Based upon EPS' investigation report, it appears the Complainant advised EPS of the privacy breach:

> On March 27, 2020, at 1047hrs, the [Complainant] called EPS very upset, stating that [the Complainant's] personal information and a report from March 8, 2020, were released to the applicant and [lawyer].

[25] EPS advised they followed up with the Complainant March 31, 2020, by telephone:

> At 1445hrs [on March 31, 2020], the [Complainant] called [EPS FOIP Co-ordinator] back. [EPS FOIP Co-ordinator] told [Complainant] about the privacy breach and that it was [EPS FOIP Co-ordinator] that released the information. [EPS FOIP Co-ordinator] gave [Complainant] my sincerest apologies, which [Complainant] accepted and said [Complainant] not faulting me as [Complainant] can tell by speaking with me that I'm genuine and didn't release the information to be malicious, and perhaps more training would be beneficial. [Complainant] was advised the records have been contained/destroyed, except for the document that was filed as an exhibit with [the Court of Queen's Bench]. [EPS FOIP Co-ordinator] also told [Complainant] the sections from [*The Queen's Bench Rules*] that this information is protected.
>
> [EPS FOIP Co-ordinator] told [Complainant] [they have] the right to complain to the IPC, and [EPS FOIP Co-ordinator] provided [Complainant] with the contact information.

[26] As noted above, the Complainant did file a breach of privacy complaint with my office regarding this matter.

[27] Although it appears the Complainant advised EPS of the breach of privacy, from information EPS provided my office, it appears EPS followed up with the Complainant in regard to this breach. In addition, EPS advised the Complainant they could file a separate complaint with my office. EPS also notified my office of the breach. Therefore, I find EPS provided appropriate notification of this breach of privacy.

Investigate the breach

[28] The next step in responding to a breach of privacy is to investigate the breach. The following are key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
- What occurred?
- How did the privacy breach occur?
- What is the applicable legislation and what specific sections are engaged?
- What safeguards, policies, and procedures were in place at the time of the privacy breach?
- Was the duty to protect met?
- Who are the affected individuals?

(Privacy Breach Guidelines, pp. 6-7)

[29] EPS FOIP Co-ordinator acknowledged to my office and the Complainant that they inappropriately provided an unredacted copy of the record to the lawyer. Furthermore, in its investigation report, EPS advised my office:

> On March 24, 2020, I received a request from a lawyer requesting an unredacted police report from March 8, 2020, regarding [the lawyer's] client … The lawyer was requesting the information to [lawyer's] office by Thursday, March 26, 2020, as they may file these materials with the Court this Friday, March 27, 2020.
>
> On March 25, 2020, [EPS FOIP Co-ordinator] gathered the information requested by the lawyer and sent the file unredacted at 1112hrs via email. As this file was no longer under investigation, and the request came from a lawyer, [EPS FOIP Co-ordinator] thought I could provide them with the information.

[30] My office asked EPS if they typically provide lawyers with information for family court. EPS advised that they typically do not provide information for family court. My office also inquired with EPS if it has any policies and/or procedures in place regarding the release of

records upon request of legal counsel. EPS advised that all disclosure requests for criminal or federal matters go through the Provincial Crown's office.

[31] Of note, EPS actually provided a redacted copy of the record to the Applicant on March 20, 2020, in response to the Applicant's access request. Therefore, based upon information provided to my office from EPS, I do not understand why EPS thought it was appropriate to provide the unredacted record five days later.

[32] Section 23.1 of LA FOIP outlines a local authorities' explicit duty to protect information in its possession or under its control. Specifically, section 23.1(b)(iii) of LA FOIP provides:

> **23.1** Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> …
> (b) protect against any reasonably anticipated:
>
> …
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control;

[33] In this case, EPS was lacking administrative safeguards that would have prevented this breach of privacy from occurring. "Administrative safeguards" are controls that focus on internal organization policies, procedures, and maintenance of security measures that protect personal information. Examples include written policies and procedures, annual training for employees, confidentiality agreements, agreements with information management service providers, auditing programs, records retention and destruction schedules, and access restrictions (*Privacy Breach Guidelines*, p. 2).

[34] From a review of what was provided to my office, it appears that the root cause of this privacy breach was human error as EPS acted too quickly to provide the lawyer the information before it confirmed that it had the authority under LA FOIP to do so. In its investigation report, EPS did not provide my office with details of how it arrived at the decision to disclose the information to the lawyer, without considering whether it had the authority to do so – although EPS acknowledged it was a mistake.

[35] I find EPS conducted an adequate investigation of this matter.

[36] My office asked EPS if it had any policies/procedures in place regarding the release of records to legal counsel. EPS, in part, advised, "… we are working on updating our policies/procedures." Therefore, from what has been provided to my office, EPS did not have the appropriate policies and procedures in place at the time the breach of privacy occurred.

[37] I find EPS failed to meet its duty to protect the Complainant's personal information when it provided an unredacted copy of the record to the lawyer.

Prevent future breaches

[38] The final step in responding to a privacy breach is to implement measures so this type of breach of privacy does not happen in the future. Therefore, local authorities must look at steps they should take to mitigate the risk:

- Can your organization create or make changes to policies and procedures relevant to this privacy breach?
- Are additional safeguards needed?
- Is additional training needed?
- Should a practice be stopped?

(Privacy Breach Guidelines, p. 7)

[39] EPS has advised my office that it is in the process of updating policies and procedures. As of the date of this Report, I understand EPS has not completed these updates and EPS did not elaborate further on the work it is doing to complete the updates. Therefore, I find EPS has begun to take steps to mitigate the risk of this type of breach happening in the future.

[40] It appears EPS released this information due to human error as EPS thought it could release the unredacted information to the lawyer because the investigation was closed. This human error may not have occurred if EPS had the appropriate policies, procedures and employee privacy training in place.

[41] Therefore, I recommend that EPS complete its policies and procedures regarding the disclosure of personal information that aligns with the requirements of section 28 of LA FOIP within the next three months.

[42] EPS should also take steps to ensure that all employees have taken privacy training and should take refresher training on an annual basis. The Access and Privacy Branch, Ministry of Justice and Attorney General (APB) can if requested, provide support to local authorities in meeting their obligations under LA FOIP. The APB developed a free, online Access and Privacy Course, which provides employees with training specifically for LA FOIP. The APB could if requested, assist EPS in how to use this course for its employees and may be able to assist EPS in exploring other privacy training and awareness opportunities.

[43] I recommend EPS require privacy training for its employees on an annual basis.

[44] As it considers these recommendations, EPS may wish to reach out to the other police services in Saskatchewan as they may have established policies, procedures and training that could assist EPS in meeting its obligations under LA FOIP.

III FINDINGS

[45] I find EPS did not contain this breach of privacy.

[46] I find EPS provided appropriate notification of this breach of privacy.

[47] I find EPS conducted an adequate investigation of this matter.

[48] I find EPS failed to meet its duty to protect the Complainant's personal information when it provided an unredacted copy of the record to the lawyer.

[49] I find EPS has begun to take steps to mitigate the risk of this type of breach happening in the future.

IV RECOMMENDATIONS

[50] I recommend EPS request again the law firm to apply to court to remove the exhibit and not cooperate with this law firm until the law firm makes the application to court to remove the exhibit.

[51] I recommend that EPS complete its policies and procedures regarding the disclosure of personal information that aligns with the requirements of section 28 of LA FOIP within the next three months.

[52] I recommend EPS require privacy training for its employees on an annual basis.

Dated at Regina, in the Province of Saskatchewan, this 3rd day of February, 2022.

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