Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 021-2023, 036-2023

Town of Hafford

June 29, 2023

Summary: The Town of Hafford (Town) proactively reported a breach of privacy to my office involving employee snooping. The Complainant was not satisfied with the response they received from the Town as an affected individual and requested my office undertake a privacy investigation. The Commissioner found that personal information is involved. While the Commissioner found the Town took adequate steps to contain the privacy breach and conducted an adequate investigation, he found the Town did not provide notification to two of the three affected individuals nor take adequate steps to prevent future breaches. The Commissioner recommended the Town provide notification to the other two affected individuals within 30 days of issuance of this Investigation Report. The Commissioner also recommended the Town develop a policy to specifically address employee snooping.

I BACKGROUND

[1] By letter dated December 8, 2022, the Complainant sent a privacy complaint to the Town of Hafford (Town). The Complainant alleged that a Town employee, for their own use, accessed information in the Complainant's home property file, as well as the property purchase information of three other properties in the Town.

[2] By letter dated December 21, 2022, the Town's response to the Complainant stated, in part:

> We the Council of the [Town] have received your complaint. We take all complaints seriously and will be investigating this matter. Thank you for bringing his to our attention.

[3] By email of January 14, 2023, the Complainant contacted my office as they were not satisfied with the response they received from the Town. My office opened IPC file 036-2023.

[4] By letter dated January 25, 2023, the Town sent another letter to the Complainant. This letter stated, in part:

> Following our investigation, we determined that your personal property file was inappropriately accessed by an employee of the [Town].
>
> …
> As stated, our investigation has revealed that your personal property file was accessed. The information that may have been accessed includes your name, contact information, and information about your property, such as date of construction, assessed value, and purchase price.

[5] On January 27, 2023, the Town proactively reported this privacy breach to my office (IPC file 021-2023). It advised:

> The incident involved a Town of Hafford administrative employee who inappropriately accessed property file records of three individuals for [their] own personal use. The information in the property files contained names, contact information, and information about their property such as date of construction, and purchase price.

[6] On January 31, 2023, my office notified the Town that my office would be undertaking an investigation of this matter and requested its investigation details.

[7] On February 21, 2023, my office notified the Town that as the Complainant brought forward a complaint, my office would be issuing an investigation report. My office also notified the Complainant that the Town proactively reported this matter to our office and my office would be issuing an investigation report.

[8] On March 2, 2023, my office received the Town's investigation details.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[9] The Town is a "local authority" pursuant to subsection 2(1)(f)(i) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). Therefore, I find I have jurisdiction to undertake this investigation.

[10] In order for LA FOIP to be engaged there must be personal information pursuant to subsection 23(1) of LA FOIP. In order to qualify as personal information, the information must 1) be about an identifiable individual; and 2) be personal in nature. Information is about an "identifiable individual" if the individual can be identified from the information (e.g., their name is provided) or if the information, when combined with information otherwise available, could reasonably allow the individual to be identified. To be "personal in nature" means the information provides something identifiable about the individual (*Guide to LA FOIP*, Chapter 6, "Protection of Privacy", updated February 27, 2023, [*Guide to LA FOIP*, Ch. 6], at pp. 39-41).

[11] When it reported the breach to my office, the Town advised the data elements included information found in property files including names, contact information, and information about their property such as date of construction and purchase price.

[12] Subsections 23(1)(b) and (e) of LA FOIP provide:

> **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:
>
> …
> (b) information that relates to the education or the criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved;
>
> …
> (e) the home or business address, home or business telephone number, fingerprints or blood type of the individual;

[13] "Financial" means of or pertaining to revenue or money matters. "Transaction" means something performed or carried out; a business agreement or exchange; any activity involving two or more persons (*Guide to LA FOIP*, Ch. 6, p. 51).

[14] "Relating to" should be given a plain but expansive meaning. The phrase should be read in its grammatical and ordinary sense. There is no need to incorporate complex requirements (such as "substantial connection") for its application, which would be inconsistent with the plain unambiguous meaning of the words of the statute. "Relating to" requires some connection between the information and the financial information (*Guide to LA FOIP*, Ch. 6, p. 51).

[15] The purchase price the Complainant paid for their home property is a financial transaction in which the Complainant was involved. This qualifies as personal information pursuant to subsection 24(1)(b) of LA FOIP.

[16] An individual's home address, telephone, facsimile (fax number) or email address is personal information under LA FOIP. Business telephone numbers and addresses would qualify as personal information only if the record was personal in nature (*Guide to LA FOIP*, Ch. 6, p. 57).

[17] The Town did not specify whether the contact information for the Complainant was their home or business contact information. However, as the contact information was there as it relates to their home property, the contact information qualifies as personal information pursuant to subsection 23(1)(e) of LA FOIP.

[18] I find that personal information is involved.

[19] The Town did not have the Complainant's consent to share their personal information, and so a privacy breach occurred. The Town is not disputing this fact, and so I will continue to assess how the Town managed the privacy breach. I note that this matter appears to be a case of employee snooping, which I will discuss later in this Investigation Report.

2. Did the Town respond appropriately to the privacy breach?

[20] A privacy breach occurs where there is an unauthorized collection, use and/or disclosure of personal information. There are also other ways a privacy breach can occur (*Guide to LA FOIP*, Ch. 6, p. 234).

[21] When assessing if a local authority properly responds to a privacy breach, my office looks at how it responded to the breach against the following four steps:

- Containment of the breach.
- Notification of affected individuals.
- Investigation of the breach.
- Steps taken to prevent future breaches.

(*Guide to LA FOIP*, Ch. 6, p. 236).

[22] I will consider these four steps in the Town's response to the breach.

Containment of the breach

[23] It is important to contain a privacy breach immediately. In other words, ensure that personal information is no longer at risk. This may involve:

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

(*Guide to LA FOIP*, Ch. 6, p. 236).

[24] In its investigation details provided to my office, the Town stated it took the following steps to contain the breach:

> The incident was a result of employee snooping. The Employee confirmed that they did not keep copies and will not use the information. The Employee has been given a disciplinary warning and all administrative staff will be provided with further LA FOIP training, privacy and confidentiality training. Hafford intends to regularly remind employees of their privacy obligations and potential consequence to reduce the likelihood of snooping in the future.
>
> …
> No records were removed, but the records were reviewed to ensure they were complete after the incident was discovered.

[25] On January 20, 2023, the Town confirmed with the employee that they did not keep copies of the information they accessed and advised that they will not use the information. In addition, the Town reviewed the files to confirm that no information had been removed. Therefore, I find the Town took adequate steps to contain the privacy breach.

Notification of affected individuals

[26] Section 28.1 of LA FOIP places an obligation on a local authority to notify individuals when their personal information has been breached and a real risk of significant harm exists for the affected individual (*Guide to LA FOIP*, Ch. 6, p. 231).

[27] Section 28.1 of LA FOIP provides:

> **28.1** A local authority shall take all reasonable steps to notify an individual of an unauthorized use or disclosure of that individual's personal information by the local authority if it is reasonable in the circumstances to believe that the incident creates a real risk of significant harm to the individual.

[28] Even where section 28.1 of LA FOIP does not apply, unless there is a compelling reason not to, local authorities should always notify affected individuals of a privacy breach.

[29] 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.
- The IPC (my office).
- The police, if criminal activity is suspected (e.g., burglary).
- The affected individuals (unless there are compelling reasons why this should not occur).

(*Guide to LA FOIP*, Ch. 6, p. 237).

[30] Notification of individuals affected by the breach should occur as soon as possible after key facts about the breach have been established. It is best to contact affected individuals directly, such as by telephone, letter or in person (*Guide to LA FOIP*, Ch. 6, p. 237).

[31] Notifications to affected individuals should include the following:

- A description of the breach (a general description of what happened).
- A detailed description of the personal information involved (e.g., name, credit card numbers, medical records, financial information, etc.).
- A description of possible types of harm that may come to the affected individual because of the privacy breach.
- Steps taken and planned to mitigate the harm and 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).
- Contact information of an individual within the 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.

(*Guide to LA FOIP*, Ch. 6, pp. 237-238)

[32] The Town proactively reported this matter to my office.

[33] Regarding the notification of the affected individuals in this matter, the Town advised:

> There were three individuals whose property files were accessed by the Employee. However, given what Hafford did to mitigate the risk, including a disciplinary letter and confirmation from the Employee that they will not misuse the information, Hafford considered that there was not a real risk that significant harm would occur, and therefore that the breach did not meet the threshold to notify the individuals.
>
> Notification was provided to the initial complainant to advise of the results of the investigation.

[34] Based on this, the Town only notified one of the affected individuals that the employee snooped in their property file.

[35] "Snooping" or the unauthorized access of personal information, occurs when employees access personal information without a need-to-know. That is, they access personal information for reasons beyond completing their job duties. Snooping is a harmful and intrusive activity that undermines the trust citizens have in a local authority's ability to maintain the confidentiality of their information (*Guide to LA FOIP*, Ch. 6, p. 334).

[36] The Complainant provided my office with a log of text communications between the Complainant and the employee that demonstrates that the employee not only snooped, but then used the information for personal gain. Of note are two text messages the employee sent the Complainant on October 27, 2022:

> 9:13 pm: And rarely do sellers get their top asking price. Even the [name removed] house came down [amount removed] grand from the original asking price on the posters.
>
> 10:23 pm: I also know you purchased it [the house] for a song. You would be making [amount removed] grand if I paid you [amount removed]. I realize you have done some renovations but even if you have put [amount removed] into it you would still be walking away with a decent profit.

[37] The employee used the information to try and negotiate a lower purchase price for the Complainant's home. This is incredibly intrusive not only to the Complainant, but also to the other affected individuals. All affected individuals deserve to know that this employee snooped in their home property files for their own personal gain.

[38] By not notifying all the affected individuals, it could look to some as if the Town is not only protecting itself from embarrassment, but also protecting the employee from being outed as a snooper. These would not be legitimate reasons to not provide notification to the other affected individuals.

[39] Therefore, I find that the Town did not provide notification to two of the three affected individuals. I recommend that within 30 days of issuance of this Investigation Report the Town provide written notification to the other two the affected individuals of this breach of privacy. The notification should include what personal information or data elements were accessed without authority, when the data elements were accessed, and the steps the Town took to address the breach including preventing future breaches of this type.

Investigation of the breach

[40] Once a breach has been contained the next step is to investigate the breach. An investigation is a methodical process of examination, inquiry, and observation including interviewing witnesses and reviewing documents (*Guide to LA FOIP*, Ch. 6, p. 238).

[41] The following are some key questions to ask during a privacy breach investigation:

- When and how did your organization learn of the privacy breach?
  - Has the privacy breach been contained?
  - What efforts has your organization made to contain the breach?

- What occurred?
  - What type of breach occurred (e.g., collection, use, disclosure, accuracy, etc.)?
  - What personal information was involved in the privacy breach?
  - When did the privacy breach occur? What are the timelines?
  - Where did the privacy breach occur?

- How did the privacy breach occur?
  - Who was involved?
  - What employees, if any, were involved with the privacy breach?
  - What privacy training have they received?
  - Who witnessed the privacy breach?
  - What factors or circumstances contributed to the privacy breach?

    - What is the root cause of the breach?

- 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?
    - Were the safeguards, policies, and procedures followed?
    - If no safeguards, policies, or procedures were in place, why not?
    - Were the individuals involved aware of the safeguards, policies, and procedures.

- Who are the affected individuals?
    - How many are there.
    - What are the risks associated to a privacy breach involving this information (e.g., is the affected individual at risk for identity theft, credit card fraud, etc.).
    - Have affected individuals been notified of the privacy breach.

(*Guide to LA FOIP*, Ch. 6, pp. 238-239).

[42] From investigation details provided to my office, it appears that the Town Council learned of this breach on December 8, 2022, when it received a letter from the Complainant. The Town advised the following in its investigation details provided to my office:

> …The written complaint was presented to the Hafford Council in camera at a meeting and the Council immediately commenced an investigation. Notice was provided to the complainant that the Council takes complaints seriously and would be investigating the matter.
>
> All Hafford files are paper based and therefore no review of access logs could be obtained.
>
> Hafford Council began with interviewing the Employee as well as any other administrative staff who may be witnesses.
>
> ….
>
> Three individuals were impacted – the information accessed was in a municipal property file and includes information such as names, contact information, and information pertaining to their property.

[43] Further, the Town advised it took the following steps to investigate the breach:

> The investigation began on December 13, 2022 when the Hafford Council reviewed the complaint in camera at a meeting, then made arrangements to interview the Employee.
>
> On December 19, 2022, the complainant called [Mayor] and was assured that the incident was being investigated.
>
> An initial interview was completed with the Employee on December 23, 2022. Following this, interviews were conducted with any administrative staff who may have observed the alleged breach.
>
> On December 28, 2022, the breach was confirmed following an interview with an administrative employee who witnessed the files accessed. The administrative employee was asked to record a written log of the dates they witnessed the Employee accessing the files.
>
> A final interview was conducted with the Employee on January 6, 2023, where the breach was admitted by the Employee and a discussion of disciplinary action took place.
>
> On January 20, 2023, a written disciplinary warning was issued to the Employee outlining the finding that the Employee improperly accessed and used personal information in Hafford's records. The written warning outlined that further privacy training would be implemented for all staff. In addition, Hafford took additional steps to confirm that the Employee would not re-use the information and has not kept any copies of the information.

[44] The Town confirmed that the employee received privacy training when they began working for the Town and that the privacy and LA FOIP training was not followed by the employee.

[45] The root cause of this privacy breach was due to the employee not following their obligations under LA FOIP to access and use personal information for a legitimate work purpose – this resulted in employee snooping. My office views employee snooping files as the most egregious type of privacy breaches. This is because the breach did not occur accidentally or through employee error. Employee snooping is an intentional act. Even worse is when an employee snoops and uses the information for potential personal gain, which in this case was to try to negotiate a lower purchase price for the Complainant's home.

[46] Although I view snooping as an egregious act, I am satisfied with the steps the Town took to investigate this matter. Therefore, I find the Town's investigation was adequate.

Take appropriate steps to prevent future breaches

[47] The most important part of responding to a privacy breach is to implement measures to prevent future breaches from occurring. This includes determining what steps can be taken to prevent a similar privacy breach in the future:

- 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?

(*Guide to LA FOIP*, Ch. 6, pp. 238-239)

[48] The Town advised my office that it has taken the following steps to prevent employee snooping breaches from occurring in the future:

> Hafford intends to review its policies and procedures to address the weakness in administrative safeguards….
>
> Hafford intends to regularly audit employees' access to personal information and make employees aware of these measures.
>
> … Hafford will provide the Employee and all other administrative employees with refresher training and at least annual training reminders thereafter relating to the importance of confidentiality and privacy and their obligations pursuant to LA FOIP.

[49] The Town also stated that it provided the employee with a written disciplinary warning as follows:

> The Employee received a written disciplinary warning outlining the finding that the Employee improperly accessed and used personal information in Hafford's records.

> The letter outlined that further misconduct may be subject to discipline up to an including termination of employment.

[50] These steps are a good start to preventing a future breach of employee snooping from occurring in the future. While the Town has taken some steps, I find that it could have done more.

[51] Section 23.1 of LA FOIP outlines the duty of a local authority to protection personal information. Section 23.1 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:
>
> (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;
>
> (b) protect against any reasonably anticipated:
>
> (i) threat or hazard to the security or integrity of the personal information in its possession or under its control;
>
> (ii) loss of the personal information in its possession or under its control; or
>
> (iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and
>
> (c) otherwise ensure compliance with this Act by its employees.

[52] For example, the Town should have sufficient administrative safeguards in place to deter employee snooping. "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 (*Guide to LA FOIP*, Ch. 6, p. 98).

[53] It does not appear that the Town has a policy in place that specifically addresses employee snooping. Therefore, I recommend the Town develop a policy to specifically address this

issue. I would note that in several cases involving employee snooping, government institutions and local authorities have fired employees for snooping. Examples of this include my office's Investigation Report 088-2022 and Investigation Report 265-2018, 266-2018. While the Town reprimanded the employee, it should have policies and procedures in place that outline what disciplinary steps the Town will take where employee snooping occurs, which should include the possibility of termination. Part of the policies and procedures could include controls such as auditing which electronic folders are accessed and by whom. Such controls would help the Town track if employees are snooping.

[54] The Town advised that it will conduct annual privacy refresher training for its employees. The Access and Privacy Branch with the Ministry of Justice and Attorney General has developed a free, online course for local authorities - *Access and Privacy Course for Saskatchewan Local Authorities*. This course provides employees with training specifically for LA FOIP and includes a section on privacy and speaks to employee snooping. As it implements annual refresher training, the Town may wish to consider this course.

III FINDINGS

[55] I find I have jurisdiction to undertake this investigation.

[56] I find that personal information is involved.

[57] I find the Town took adequate steps to contain the privacy breach.

[58] I find that the Town did not provide notification to two of the three affected individuals.

[59] I find the Town's investigation was adequate.

[60] I find the Town has taken some adequate steps to prevent future employee snooping breaches of privacy, but could take some additional steps.

IV RECOMMENDATIONS

[61] I recommend that within 30 days of issuance of this Investigation Report the Town provide written notification to the other two affected individuals of this breach of privacy. The notification should include what personal information or data elements were accessed without authority, when the data elements were accessed, and the steps the Town took to address the breach including preventing future ones of this type.

[62] I recommend the Town develop a policy to specifically address employee snooping.

Dated at Regina, in the Province of Saskatchewan, this 29th day of June, 2023.

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