Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 041-2021

Ministry of Justice and Attorney General

May 4, 2022

Summary: The Ministry of Justice and Attorney General (Justice) received a complaint alleging that Justice had, without proper authority, disclosed the Complainant's personal information to a collection agency. Justice responded to the Complainant, stating that no privacy breach had occurred because it had authority to disclose the Complainant's personal information pursuant to sections 29(2)(a), (e), (f)(i) and (u) of *The Freedom of Information and Protection of Privacy Act* (FOIP) and section 16(h.3) of *The Freedom of Information and Protection of Privacy Regulations.* The Complainant requested the Commissioner investigate. The Commissioner found that Justice had authority to disclose the Complainant's personal information to the collection agency pursuant to section 29(2)(a) of FOIP. The Commissioner recommended that as a best practice Justice review its agreements, policies and procedures to ensure that need-to-know and data minimization principles are adhered to when disclosing personal information to collection agencies.

I BACKGROUND

[1] On January 21, 2021, the Complainant contacted the Ministry of Justice and Attorney General (Justice) alleging that Justice had breached their privacy, when it disclosed their personal information to a collection agency.

[2] On February 19, 2021, Justice responded to the Complainant indicating that it had authority to disclose the Complainant's personal information to the collection agency pursuant to section 29(2)(f)(i) of *The Freedom of Information and Protection of Privacy Act* (FOIP). Justice indicated that no privacy breach had occurred.

[3] On February 23, 2021, the Complainant requested my office investigate Justice's authority to disclose their personal information to the collection agency.

[4] On March 3, 2021, my office notified Justice and the Complainant of my office's intention to undertake an investigation. My office requested a copy of Justice's internal investigation report regarding the matter. My office also invited the Complainant to provide a submission with any further details regarding the alleged breach of privacy.

[5] On April 4, 2021, the Complainant provided a submission to my office and on July 5, 2021, Justice provided its internal investigation report to my office.

II DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[6] Justice qualifies as a "government institution" pursuant to section 2(1)(d)(i) of FOIP. Therefore, I have jurisdiction to conduct this investigation.

2. Is the Complainant's personal information involved?

[7] In order for FOIP to be engaged in a privacy breach, there must be personal information involved, as defined by section 24(1) of FOIP.

[8] In its internal investigation report to my office, Justice provided background and explained that its Fine Collection Branch (FCB) was responsible for the collection of fines pursuant to *The Summary Offences Procedure Act, 1990*. The FCB uses a secure system, the Criminal Justice Information Management System (CJIMS), to manage the enforcement of fines. CJIMS tracks whether the summary offence tickets (SOTs) have been paid and contains the personal information that was collected by the police at the time the ticket was issued. If the SOT remains unpaid after a specific period of time, CJIMS keeps track of the outstanding amount of the fine and any late fees that have been applied.

[9] Justice further explained that it sends one Notice of Conviction letter and two enforcement letters to an individual, requesting payment of the fines and any late fees. If an individual does not respond to either of the enforcement letters, then it shares the individual's information with a collection agency (Partners in Credit), which is then responsible to collect the outstanding fine amount on Justice's behalf. Justice explained that it has an agreement with the collection agency for this service.

[10] According to its process, Justice mailed one Notice of Conviction letter to the Complainant dated July 6, 2020, followed by two enforcement letters dated October 18, 2020 and November 8, 2020. As the Complainant did not respond to any of these letters, Justice indicated that it provided the Complainant's information to the collection agency on November 22, 2020 for the purpose of collecting the outstanding fine amount.

[11] In its internal investigation report to my office, Justice listed the following data elements that it disclosed to the collection agency:

- Name
- Criminal history – amount of the fine, offence charged, offence date, the date the fine was due, court location and court office
- Information number
- Date of birth – age
- Gender
- Driver's license customer number/ personal identification card (PIC) number
- Province that issued the driver's license
- Home address

[12] I note that the data elements listed above would qualify as personal information as defined by sections 24(1)(a), (b), (d), (e) and (k)(i) of FOIP, which provide as follows:

> **24**(1) Subject to sections (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 or origin of the individual;

> (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;
> …
>
> (d) any identifying number, symbol or other particular assigned to the individual, other than the individual's health services number as defined in *The Health Information Protection Act*;
>
> (e) the home or business address, home or business telephone number or fingerprints of the individual;
> …
>
> (k) the name of the individual where:
>
> (i) it appears with other personal information that relates to the individual; or
> …

[13] Therefore, I find that the Complainant's personal information is involved pursuant to sections 24(1)(a), (b), (d), (e) and (k)(i) of FOIP. As such, FOIP is engaged and the privacy rules outlined in Part IV of FOIP will guide this investigation.

3. Did Justice have authority to disclose the Complainant's personal information to the collection agency?

[14] Once personal information is established, the next step is to consider which of the three primary privacy activities are engaged, i.e. collection, use and/or disclosure. Finally, authority for the privacy activity would need to be established. Where there is no authority established, a privacy breach has occurred.

[15] "Disclosure" means to share personal information with a separate entity, not a division or branch of a government institution in possession or control of that record/information (Investigation Report F-2014-002 at para [53]).

[16] On November 22, 2020, Justice shared the Complainant's personal information with the collection agency . This constituted a disclosure.

[17] Section 29(1) of FOIP establishes that a government institution may only disclose personal information with the consent of an individual or without consent if one of the sections of 29(2) of FOIP or section 30 of FOIP apply. Section 29(1) of FOIP 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.

[18] In its internal investigation report to my office, Justice asserted that it had authority to disclose the Complainant's personal information to the collection agency pursuant to sections 29(2)(a), (e), (f)(i) and (u) of FOIP and section 16(h.3) of *The Freedom of Information and Protection of Privacy Regulations* (FOIP Regulations).

[19] I will begin by considering section 29(2)(a) of FOIP which provides:

> **29**(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed:
>
> (a) for the purpose for which the information was obtained or compiled by the government institution or for a use that is consistent with that purpose;

[20] In Investigation Report 059-2018, my office considered the application of section 28(2)(a) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP), which is substantially similar to section 29(2)(a) of FOIP. In that report, my office established the following criteria where the provision is relied upon for an authorized disclosure:

> [18] In order to rely on section 28(2)(a) of LA FOIP, "purpose" and "consistent purpose" are important concepts to understand. Service Alberta's *FOIP Guidelines and Practices* (2009) at page 260, states the following:
>
> The "purpose" means the purpose of which the information was collected… A public body can use the information for that purpose. Typical purposes include the administration of a particular program, the delivery of a service and other directly related activities.
>
> A "consistent purpose" is one that has a direct and reasonable connection to the original purpose and that is necessary for performing the statutory duties of, or

> for operating a legally authorized program of, the public body that uses the information…
>
> [19] The former federal Privacy Commissioner has similarly stated in Expectations: *A Guide for Submitting Privacy Impact Assessments* to the Office of the Privacy Commissioner of Canada at page 9, that "…For a use or disclosure to be consistent, it must have a reasonable and direct connection to the original purpose for which it was obtained or compiled."…

[21] In its internal investigation report, Justice asserted that the personal information was originally obtained for the purpose of its fine collection program. Its FCB division is responsible for managing the enforcement and collection of fines and penalties imposed pursuant to section 57(2) of *The Summary Offences Procedure Act, 1990* (SOPA).

[22] Subsection 57(2) of SOPA provides:

> **57**(2) Subject to subsections (3) to (6) and a provision in any other Act respecting fines or penalties, any fines or other penalties imposed pursuant to an offence governed by this Act belong to the Crown in right of Saskatchewan.

[23] Upon review of the letters and the agreement between Justice and the collection agency, my office noted that Justice appeared to have followed its normal process for the enforcement and collection of fines in this case. Furthermore, its agreement with the collection agency, clearly listed the service terms and obligations of the collection agency. One of the obligations of the collection agency was to "… collect on a variety of different accounts (i.e. individuals and commercial) across Canada…".

[24] It appears that Justice disclosed the Complainant's personal information to the collection agency for the purpose of collecting the unpaid fine. This is a purpose consistent with why the personal information was originally obtained or compiled by Justice. Disclosure of the Complainant's personal information by the FCB division was necessary for performing the statutory duties of its program, i.e. managing the enforcement and collection of fines. Therefore, I find Justice had authority to disclose the Complainant's personal information to the collection agency pursuant to section 29(2)(a) of FOIP.

[25] As I have found that Justice had authority to disclose the Complainant's personal information to the collection agency for the purposes noted above, I do not need to consider the application of sections 29(2)(e), (f)(i) and (u) of FOIP and section 16(h.3) of the FOIP Regulations in this matter.

[26] I note that while a provision in FOIP provides a government institution with the authority to disclose personal information, it does not mean that the government institution does not need to take both the need-to-know and data minimization principles into consideration when dealing with personal information. A privacy breach can still occur if the government institution discloses more personal information than is necessary, or personal information is shared without a legitimate need-to-know.

[27] The need-to-know and data-minimization principles are underlying principles of FOIP and are defined as follows:

> - ***Need-to-know***: means that only those with a legitimate need-to-know for the purpose of delivering mandated services should have access to personal information.
>
> - ***Data minimization***: means that government institutions should always collect, use and/or disclose the least amount of personal information necessary for the purpose.
>
> (Investigation Report 133-2015 at paras [18] to [19])

[28] I recommend that as a best practice, Justice review its agreements, policies and procedures to ensure that need-to-know and data minimization principles are adhered to when disclosing personal information to collection agencies.

III FINDINGS

[29] I find that the Complainant's personal information is involved pursuant to sections 24(1)(a), (b), (d), (e) and (k)(i) of FOIP.

[30] I find that Justice had authority to disclose the Complainant's personal information to the collection agency pursuant to section 29(2)(a) of FOIP.

IV RECOMMENDATION

[31] I recommend that as a best practice, Justice review its agreements, policies and procedures to ensure that need-to-know and data minimization principles are adhered to when disclosing personal information to collection agencies.

Dated at Regina, in the Province of Saskatchewan, this 4th day of May, 2022.

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