Office of the
Saskatchewan Information
and Privacy Commissioner

REVIEW REPORT 210-2023

Saskatoon Police Service

December 19, 2023

Summary: The Applicant submitted an access to information request to the Saskatoon Police Service (SPS). SPS withheld portions of the records pursuant to subsections 14(1)(j) and 28(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP). The Applicant was not satisfied and requested that the Commissioner undertake a review of the exemptions claimed. The Commissioner found that SPS properly applied subsection 14(1)(j) of LA FOIP. The Commissioner also found that SPS did not properly apply subsection 28(1) of LA FOIP. The Commissioner recommended that SPS continue to withhold or release the information in the records accordingly within 30 days of the issuance of this Report.

I BACKGROUND

[1] On August 12, 2023, the Saskatoon Police Service (SPS) received the Applicant's access to information request, which stated:

> I am seeking a list, in CSV format, of all calls for service, general occurrence or other reports in your records system [address redacted]. This search is only to be done digitally and does not require a search of the hard archives.
>
> The record fields (or 'header' fields) I am seeking to be returned should include: Main Offence, Operational Status, Reported On, Approved On, Occurred On, Submitted By, CCJS Status, Offences committed, Location type.
>
> The date range for this search is from 1982 to 2023.

[2] On September 7, 2023, SPS issued its section 7 decision letter to the Applicant, advising that portions of the responsive records were being withheld pursuant to subsections 14(1)(j) and 28(1) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

[3] On September 8, 2023, the Applicant requested that my office undertake a review of SPS' decision to withhold portions of the records pursuant to subsections 14(1)(j) and 28(1) of LA FOIP.

[4] On October 4, 2023, my office notified SPS and the Applicant of my office's intention to undertake a review.

[5] On October 4, 2023, the Applicant responded indicating that they would not be providing a submission. On November 30, 2023, SPS provided its submission.

II RECORDS AT ISSUE

[6] At issue are two spreadsheets containing the CSV data requested by the Applicant. Spreadsheet #1 is referred to as "Calls for Service". Spreadsheet #2 is referred to as "General Occurrence Reports".

[7] SPS withheld all call codes under the "Initial Call Type" and "Final Call Type" columns from Spreadsheet #1 pursuant to subsection 14(1)(j) of LA FOIP. The 206 cells under the "Initial Call Type" column had a call code withheld from each of the cells. Call codes were in 57 of the cells under the "Final Call Type" column which were withheld in full.

[8] SPS withheld the date in 41 cells out of 115 under the "Occurred On" column from Spreadsheet #2 pursuant to subsection 28(1) of LA FOIP.

III DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[9] SPS qualifies as a "local authority" pursuant to subsection 2(1)(f)(viii.1) of LA FOIP. Therefore, I have jurisdiction to conduct this review.

2. Did SPS properly apply subsection 14(1)(j) of LA FOIP?

[10] As SPS applied subsection 14(1)(j) of LA FOIP to all call codes under the "Initial Call Type" and "Final Call Type" columns from Spreadsheet #1.

[11] Subsection 14(1)(j) of LA FOIP provides:

> **14**(1) A head may refuse to give access to a record, the release of which could:
>
> …
> (j) facilitate the commission of an offence or tend to impede the detection of an offence;

[12] My office's *Guide to LA FOIP*, Chapter 4, "Exemptions from the Right of Access" (*Guide to LA FOIP*, Ch. 4) at page 75 provides that subsection 14(1)(j) of LA FOIP is a discretionary harm-based exemption. It permits refusal of access in situations where release of a record could facilitate the commission of an offence or impedes the detection of one.

[13] The *Guide to LA FOIP*, Ch. 4 at page 75 and 76, provides that the following two-part test can be applied:

1. Does the information constitute law enforcement intelligence information?
2. Could disclosure reveal law enforcement intelligence information?

[14] In its submission to my office, SPS stated that subsection 14(1)(j) of LA FOIP was used to withhold "SPS dispatch (i.e. "ten-codes")" as follows:

> The use of ten-codes by law enforcement personnel is used as a means of communication that conveys a specific message without publicly identifying its true meaning. In Saskatchewan, each police service maintains an individual list of ten-codes only used by one specific police service, with the exception of standardized ten-codes such as 10-4 (understood/message received).
>
> …
> With the objective of officer and public safety, the SPS has utilized encryption methods in order to protect radio transmissions from being intercepted. However, should these encryption methods be breached, the ten-codes would maintain a level of security over the communications of members. The IPC has upheld the SPS' use of this subsection for this specific purpose in Review Reports 037-2018, 023-2019/-098-2019 and 353-2019.

[15] In my office's Review Reports 037-2018, 023-2019, 098-2019, 353-2019 and 077-2023, also concerning SPS, my office found that "ten codes" are law enforcement intelligence information, and that disclosing them could facilitate the commission of an offence, which would reveal law enforcement intelligence. I take the same approach in this matter and find that as both parts of the test are met, SPS properly applied subsection 14(1)(j) of LA FOIP. I recommend that SPS continue to withhold the "ten codes" from the record pursuant to subsection 14(1)(j) of LA FOIP.

3. Did SPS properly apply subsection 28(1) of LA FOIP?

[16] SPS applied subsection 28(1) of LA FOIP to withhold some of the dates under the "Occurred On" column from Spreadsheet #2.

[17] Subsection 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.

[18] The *Guide to LA FOIP*, Chapter 6, "Protection of Privacy" (*Guide to LA FOIP*, Ch. 6) at page 163 provides that section 28 of LA FOIP prohibits the disclosure of personal information, unless the individual about whom the information pertains, consents to its disclosure or if the disclosure without consent is authorized by one of the enumerated

subsections of 28(2) or section 29 of LA FOIP. Section 28 of LA FOIP only applies to personal information as defined by section 23 of LA FOIP.

[19] SPS' submission provides, in part, as follows:

> The address that the applicant requested information about is a school in [location redacted] that has been the subject of immense media scrutiny due to allegations… There is a concern that by releasing the date of the offences, the victims or accused may become identifiable through information that is already available, such as through yearbooks and the small enrollment size of the school over time. This concern is compounded by the applicant's six FOIP requests in relation to the school and the applicant's own admission that [they are] partaking in "data journalism", though the applicant is not a member of the media and has not been personally involved in any of the police files…
>
> The meaning of the "reasonable expectation" standard can be found in the Supreme Court of Canada's interpretation of the similar phrase "could reasonable [sic] be expected", as provided in *Merck Frosst Canada Ltd. V. Canada (Health)*:
>
> > [204] ... **The words "could reasonably be expected" "refer to an expectation for which is real and substantial grounds exist when looked at objectively**": *Watt v. Forests NSW* [(August 29, 2007)], Doc. 063292 (Australia Admin. Appeals Trib.)], [2007] NSWADT 197 at para. 120. **On the other hand, what is at issue is risk of future harm that depends on how future uncertain events unfold.** Thus, requiring a third party (or, in other provisions, the government) to prove that harm is more likely than not to occur would impose in many cases an impossible standard of proof.
> >
> > [Emphasis added in SPS submission]
>
> It is not believed that the applicant has a nefarious purpose for making the requests, however there is a concern that if the disclosed information is made public, the information could be used to data match and identify victims or accused in the occurrences. As previously noted, victims of the offences may be identifiable through quasi-identifiers from the dates of the occurrences through publicly available records such as yearbooks, which show class sizes of an average 10 students.
>
> …
> The SPS released dated [sic] in relation to other calls for service and occurrences at the requested address, as the potential impact on privacy or identifying of victims was not of concern. However, as noted above, the probability and degree of injury, should individuals become identifiable through the requested information, was high enough to not allow disclosure.

[20] The *Guide to LA FOIP*, Ch. 6 at pages 26, 28, 39 and 40, provides the following definitions about quasi-identifiers and if the information is about an identifiable individual:

> - "Indirect or quasi-identifiers" are fields of information that may be used on their own or in combination with other indirect or quasi-identifiers, or other information, to indirectly identify an individual. They include information such as gender, marital status, race, ethnic origin, postal code or other location information, significant dates, or one's profession. Some indirect or quasi-identifiers may be more likely to lead to the re-identification of individuals in a data set due to their rare occurrence. Characteristics which are highly uncommon in the population or in the data set, such as an unusual occupation or medical diagnosis, can increase the likelihood of the identity of an individual being revealed.
>
> …
> Examples of quasi-identifiers can include sex, date of birth or age, geo-codes, first language, ethnic origin, aboriginal identity, total years of schooling, marital status, criminal history, total income, visible minority status, profession, health event dates, health-related codes, country of birth, birth weight, and birth plurality.
>
> Sufficient quasi-identifiers make it possible to identify an individual even in absence of a name, either on their own or in combination.
>
> …
> Information is about an identifiable individual if:
>
> - The individual can be identified from the information (e.g., name, where they live); or
>
> - The information, when combined with information otherwise available, could reasonably be expected to allow the individual to be identified.
>
> - "Identifiable" means that it must be reasonable to expect that an individual may be identified if the information were disclosed. The information must be reasonably be capable of identifying particular individuals because it either directly identifies a person or enables an accurate inference to be made as to their identity when combined with other available sources of information (data linking) or due to the context of the information in the record.

[21] In the current records at issue, SPS withheld 41 cells out of 115 under the "Occurred On" column. The cells in this record that were released to the Applicant provide data regarding the occurrences at this location including the date the occurrence was reported, the type of offence (suspicious activity, sexual assault, assault, sexual interference, sexual exploitation, etc.), the operational status (founded (open), inactive (closed), cleared by

charge/otherwise (closed)), CCJS Status [Canadian Centre for Justice Statistics Status] (unfounded, founded not cleared, charged, still under investigation, insufficient evidence to proceed, victim/complainant declines to proceed, etc.). SPS noted that it had released some dates in relation to other calls for services or occurrences, but not others due to the potential of identifying victims. Based on a review of the record, it appears SPS released the date of occurrences based on the level of sensitivity of the offence.

[22] My office has considered quasi-identifiers in previous reports (e.g., Investigation Report 114-2017 and Review Report F-2014-005) as ways to narrow down an identity, in the absence of a name, given a combination of data elements. Review Report F-2014-005 dealt with an access request for professional misconduct or incompetence of teachers. In that Report, it was found that the name of the specific school, classes taught, extra-curricular responsibilities and work email addresses should be withheld pursuant to subsection 29(1) of *The Freedom of Information and Protection of Privacy Act*. In Investigation Report 114-2017, it provided that even without the release of the name of the individual, quasi-identifiers in that file included that there was a harassment investigation against the Complainant in the town of Ituna and dates which could narrow down the timeframe. In that report, it was found that in a small town, such as Ituna, "it is highly probable that most, if not all, residents would be able to figure out who the Complainant was." Additionally, it was noted that with the quasi-identifiers, it would be possible to determine the identity of the Complainant through publicly available sources. Factors in these matters weighed favourably in a reasonable expectation that an individual could be identified.

[23] In Information and Privacy Commissioner of Ontario (ON IPC) Order PO-4401, an Applicant had requested data from Ontario Health for data related to patients who died while on waiting lists for the fiscal year of 2020-2021. In that review, the ON IPC considered if a table containing diagnostic scan or procedure, decision to treat date, scheduled procedure date, order/referral received date, procedure no longer require date (death date) and procedure no longer required reason. In that Order, it provided the following regarding what it called the key issue of "identifiability":

[26] The appellant does not seek the names of any of the patients who died while on a waiting list. He also does not seek their sex, ethnic background, postal code or address, or information that would identify the doctor or medical facility involved (or would have been involved) in their care before passing away. Rather, he sees his request as one for "anonymous data," and emphasizes the importance of maintaining patient confidentiality. He also notes that Ontario hospitals (and other provinces) that serve much smaller populations provided similar data breakdowns without any issues.

[27] OH submits that what the appellant seeks is "by definition, not anonymous patient information, given that the patient details that would be disclosed risk the re-identification of such individuals."

…

[31] The crux of OH's position in this appeal is that, "given the data attributes that would be disclosed as part of this release (including date of death, procedure dates, and details of the service)," there is a risk of re-identification of individuals who were on a waiting list by a third party (such as a family member, neighbour, or business colleague) who is aware of information such as the date of death and, for example, the fact that the individual was to have a procedure (or the date of that procedure). OH notes that its data de-identification guidelines as a prescribed entity under PHIPA require it to consider "Acquaintance Quasi-Identifiers" (AQIs). AQIs refer to personal identifiers that relate to information that indirectly identifies an individual but is only knowable to those who may be acquainted with an individual contained in a data set. **OH submits that the appellant, who publishes "record-level information" to his website, would have these quasi-identifiers available to anyone, such that an individual on the Wait Times Information System may be identified as a result.**

[32] In my view, these arguments are speculative at best, and do not sufficiently consider the nature of the information that will be in the table that OH will create (and, just as importantly, what will not be in the table). Nor do these arguments sufficiently address the number of entries in the table, and the limitations of the information itself.

[33] In considering whether unnamed patients can be identified from the information in the record, I am mindful of PHIPA Decision 82, which found that a hospital had relied too heavily on the fact that it had not named a patient to argue that no personal health information was in its public statement about a matter. In those circumstances, there was other publicly available information that showed that a patient was identifiable (and indeed already identified by a journalist linking certain information in the public realm to the hospital's statements about the unnamed patient).

[34] However, in the appeal before me, **there is insufficient evidence about specific publicly available information that could be used, along with the information in the record, to identify any individual in the table that OH will create. OH submits that a third party that has already received information about a group of patients and is seeking further information about their identities or clinical outcomes could use key dates about an individual to cross-reference data sets. It is not clear whether OH is referring to the appellant (who has received aggregate data), but**

the evidence does not establish that he is seeking their identities (it indicates the opposite). In any event, OH does not specify what data sets he, or any other third party, may cross-reference the information in the responsive record with, so I do not accept this argument as reasonable or persuasive.

[35] I acknowledge that there will be sub-pools of information from the total of 7787 lines of data. For example, individuals who all died on the same day would form a sub-pool of entries. If the identities of the deceased and dates of their deaths are otherwise in the public domain, and if the sub-pool is very small, one might theoretically be able to guess what individual had what condition. However, what would not be publicly known is whether any particular deceased individual was awaiting a particular surgery. In these circumstances I find the risk of re-identification from public knowledge of dates of death to be remote.

[36] The IPC has also considered similar arguments about identifiability of unnamed individuals as those presented in this appeal.

[37] Former Commissioner Brian Beamish considered the issue of identifiability resulting from combining information in the public realm with the information at issue in Orders MO-2337 and PO-2892. In those orders, the former Commissioner acknowledged that there will be situations where a limited number of people may already be independently aware of individuals referred to in records where the names would be redacted. He determined that this does not affect a decision to disclose such records under the applicable public sector statutes in those orders, since **disclosure of the records without the names would not itself result in the identification of the unnamed individuals to the vast number of people who are unaware of the individuals' identities.**

[38] In Order PO-3643, the IPC considered whether the disclosure of statistical information related to suicides in Ontario hospitals and psychiatric facilities could be linked to information known to others in a manner that would identify the individuals reflected in the statistics. In my view, the following statement by the IPC is relevant to considering the arguments before me:

> **Identifiability must result from the disclosure of the information at issue on its own or in combination with other available information. Identifiability does not result simply because someone who already knows the information**, in this case a friend or family member of an individual who committed suicide and who already knows about the individual's suicide, recognizes a statistic in the form of a year and a facility as representing the deceased individual's suicide. Obviously, there are people who know about these suicides by virtue of their relationship with or knowledge of a deceased individual, including the staff at the facilities who assisted the deceased individual. However, **the prior personal knowledge of a few does not establish identifiability in the general public when the withheld information does not disclose any personal information** about the deceased.

> [39] Order PO-4272 followed this reasoning, that **identifiability must flow from the information itself, not from prior personal knowledge being reflected in the records.** In that appeal, the institution argued that it is reasonably foreseeable that people connected to a patient whose treatment is reflected in a report might have information in their knowledge that could be combined with the information in the report in a way that would result in the identification of that particular patient. The IPC held that **any information that might be known to individuals as a result of their personal connection to the patient is not information that can be said to exist generally in the public realm, and that it is information that would be known to a very limited number of individuals. As a result, the IPC did not accept that information that is already known as a result of a personal connection to the patient establishes identifiability in the general public when the withheld information itself does not, on its own or in association with other publicly available information, disclose any personal information about the patient.**
>
> [40] Here, I am not satisfied that release of the information at issue would enable the identification of any patient, except to those who are already aware of it through a personal connection. I agree with Commissioner Beamish that this does not render the information "identifying information."
>
> [Emphasis added]

[24] SPS indicated that the Applicant has submitted multiple access to information requests related to the school which has also had a lot of media attention. Some of the media attention focused on the size of the school and number of former students who attended or want to be part of the class-action lawsuit against it. New articles, for example, have stated the number of students who have attended from the 1980s to today. SPS is concerned that the Applicant could combine known data elements such as these, along with the withheld occurrence dates to identify victims or the accused. SPS, though, has not stated what other specific types of data elements the Applicant has already accessed or may know that could help them identify anyone.

[25] In the records at issue, there are no data elements such as age, grade of the victim or gender, which are all identifiers that would make it easier to identify someone. Previous reports from my office have found that quasi-identifiers can lead to identify an individual in the absence of a name, but those other identifiers need to be combined in such a way that an identity could reasonably be ascertained. As in ON IPC Order PO-4401, "identifiability must flow from the information itself, not from prior personal knowledge being reflected

in the records." SPS has not provided my office with enough detail to support its argument that releasing the occurrence dates in question could reasonably identify either a former student or the accused. As the information must relate to an identifiable individual in order to qualify as personal information pursuant to subsection 23(1) of LA FOIP, I am not convinced that the information at question qualifies as personal information.

[26] As such, I find that SPS did not properly apply subsection 28(1) of LA FOIP to the record. I recommend SPS release the redacted portions of spreadsheet #2 within 30 days of the issuance of this Report.

IV FINDINGS

[27] I find that I have jurisdiction to conduct this review.

[28] I find that SPS properly applied subsection 14(1)(j) of LA FOIP to the record.

[29] I find that SPS has not properly applied subsection 28(1) of LA FOIP to the record.

V RECOMMENDATIONS

[30] I recommend SPS continue to withhold the redacted portions of spreadsheet #1.

[31] I recommend SPS release the redacted portions of spreadsheet #2 within 30 days of the issuance of this Report.

Dated at Regina, in the Province of Saskatchewan, this 19th day of December, 2023.

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