Office of the
Saskatchewan Information
and Privacy Commissioner

REVIEW REPORT 160-2024

Regina Police Service

October 15, 2024

Summary: The Applicant submitted an access to information request to the Regina Police Service (RPS) for video of their arrest in the lobby of the RPS headquarters. The RPS identified 20 videos responsive to the Applicant's access request but denied the Applicant access to all of the videos. The RPS cited subsection 14(1)(m) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) as its reason. The Applicant requested a review by the A/Commissioner of RPS' decision. In the review, the Applicant specified they were seeking only the videos of their arrest, and not videos of them in other parts of the building. The A/Commissioner found that RPS did not properly apply subsection 14(1)(m) of LA FOIP. The A/Commissioner recommended that RPS release eight of the videos that recorded the Applicant's arrest to the Applicant within 30 days of issuance of this Report.

I BACKGROUND

[1] On April 30, 2024, the Regina Police Service (RPS) received the following access to information request from the Applicant:

> I require a copy of the video of my arrest. Which was on October 11, 2023 and on your own security cameras at the police station. Where my arm was broken by one of the arresting officers as I was already on the ground. And now I have a permanent problem with my arm.

[2] In a letter dated May 31, 2024, RPS responded to the Applicant. RPS indicated it was withholding the records in full pursuant to subsection 14(1)(m) of *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP).

[3] On June 13, 2024, my office received the Applicant's request for review.

[4] On June 20, 2024, my office notified both RPS and the Applicant that my office would be undertaking a review.

[5] On August 22, 2024, RPS provided its submission to my office.

[6] The Applicant did not provide a submission.

II RECORDS AT ISSUE

[7] The RPS withheld 20 videos in full from the Applicant. Eight of the videos are footage of the Applicant in the lobby where they were arrested. The remaining 12 videos are of the Applicant where they appeared in other parts of RPS headquarters after their arrest.

III DISCUSSION OF THE ISSUES

1. Do I have jurisdiction?

[8] RPS is a "local authority" as defined by subsection 2(1)(f)(viii.1) of LA FOIP. Therefore, I find that I have jurisdiction to conduct this review.

2. Did RPS properly apply subsection 14(1)(m) of LA FOIP?

[9] RPS withheld all 20 videos from the Applicant, in full, pursuant to subsection 14(1)(m) of LA FOIP. Subsection 14(1)(m) of LA FOIP provides:

> **14**(1) A head may refuse to give access to a record, the release of which could:
>
> ...
> (m) reveal the security arrangements of particular vehicles, buildings or other structures or systems, including computer or communication systems, or methods employed to protect those vehicles, buildings, structures or systems.

[10] My office uses the following test to determine if subsection 14(1)(m) of LA FOIP applies. Only one of the questions needs to be answered in the affirmative in order for my office to find that subsection 14(1)(m) of LA FOIP applies, although both questions may be answered in the affirmative.

1. Could the release of information reveal security arrangements (of particular vehicles, buildings, other structures or systems)?

2. Could the release of information reveal security methods employed to protect particular vehicles, buildings, other structures, or systems?

(*Guide to LA FOIP*, Chapter 4: "Exemptions from the Right of Access", updated October 18, 2023 [*Guide to LA FOIP*, Ch. 4], p. 90)

[11] Before I proceed with my analysis of subsection 14(1)(m) of LA FOIP, I note that the Applicant specified what video footage they were seeking. They said in their submission:

> I do not want hours of video of myself in the building prior to or leading up to my arrest. I only acquire [sic] a few minutes of video and thats [sic] seconds before my arrest to the point I am escorted out of the building.

[12] As such, I will only consider the eight videos that are footage from one camera located in the lobby. The other 12 videos are footage from other parts of RPS headquarters, which the Applicant is not interested in.

[13] Even though only one question needs to be answered in the affirmative, RPS provided my office with arguments for both questions. Below is my analysis to determine if either question can be answered in the affirmative.

1. Could the release of information reveal security arrangements (of particular vehicles, buildings, other structures or systems)?

[14] Page 90 of the *Guide to LA FOIP*, Ch. 4, provides the following definitions:

- "Reveal" means to make known; cause or allow to be seen.
- "Security" means a state of safety or physical integrity.

- "Other structures or systems" includes computer and communication systems.

[15] Further, section 14 of LA FOIP uses the word "could" instead of "could reasonably be expected to" as seen in other provisions of LA FOIP. The threshold for "could" is somewhat lower than a reasonable expectation. The requirement for "could" is simply that the release of the information "could" have the specified result. There would still have to be a basis for the assertion. If it is fanciful or exceedingly remote, the exemption should not be invoked (*Guide to LA FOIP*, Ch. 4, p. 91).

[16] In its submission, RPS indicated that its position is that providing access to the videos would reveal security arrangements of the main lobby of the RPS headquarters. RPS indicated it has signage to notify the public there are cameras on-site. However, RPS indicated that the exact locations of the cameras are not made public for the following reasons:

- We aware [sic] that public knows there are cameras on sight [sic] as we have signage around the station to notify. However the exact locations are not made public for the following reasons:

    i. Informed Intruders
        1. When the locations of security cameras are publicly known, potential intruders can plan their activities with the advantage of knowing which areas are monitored and which are not. This allows them to avoid camera-covered zones making the system less effective at deterring or capturing illicit activity. ****

    ii. Exposure of Unmonitored Zones
        1. Security cameras are typically placed in locations to cover vulnerable areas. If these locations are revealed, intruders can identify which parts of the building are not under surveillance and focus their efforts on these less-protected zones.

    iii. Interference of Surveillance plans
        1. Security systems are often designed with a combination of visible and hidden cameras to create a comprehensive surveillance network. Publicly revealing camera locations disrupts this strategy by decreasing the element of surprise. Intruders can exploit this information to avoid detection or to gather information about security responses.

> iv. Increased Risk of Camera Damage
>
> 1. Public knowledge of camera locations also increases the risk of camera vandalism. Individual's intent on criminal activities might attempt to disable or damage cameras to prevent them from detected [sic].

[17] Also, in its submission, RPS indicated that the Applicant had broken into RPS headquarters and went undetected for a significant period of time before they were arrested. As such, RPS asserted that it had concerns about the Applicant's knowledge of the layout of the building and added that providing the Applicant with information about camera angles and locations "could affect security of the Regina Police Service".

[18] In summary, RPS' arguments for the first question appear to assert that the release of the information would reveal security arrangements of RPS headquarters. Specifically, it would reveal which areas of the headquarters are monitored by video surveillance and which areas are not, which could help inform intruders on how to go about undetected. Further, by disclosing the videos to the Applicant (who had been in the building), it asserted that the Applicant would know precisely what parts of the building are monitored and which parts aren't.

[19] RPS' argument is premised on disclosing video footage from different areas of headquarters. However, since the Applicant has clarified that they are only seeking video footage from the lobby, I am only considering the eight videos recorded by one camera located in the lobby in this review.

[20] In Order PO-2358, Ontario's Office of the Information and Privacy Commissioner (ON IPC) considered a case involving an access request to Ontario Lottery and Gaming Corporation (OLGC) for videotape of an incident at a casino. OLGC was concerned that disclosure of the video tape would reveal the level and kind of surveillance, how cameras scan the floor, the extent of coverage, what a camera is viewing at a given time and gaps in coverage. Therefore, OLGC withheld the videotape pursuant to subsection 14(1)(i) of Ontario's *Freedom of Information and Protection of Privacy Act* (ON FIPPA), which is similar to subsection 14(1)(m) of LA FOIP. However, when the ON IPC reviewed the

videotape in question, it concluded that the contents of the videotape would not be able to draw accurate inferences about the level and kind of surveillance at the casino as follows:

> It is apparent that the OLGC's concerns are not just that viewing the videotape would reveal the existence and location of cameras. Its representations indicate that it is also concerned about the revelation of the level and kind of surveillance, how the cameras scan the floor, the extent of coverage, what the camera is viewing at a given time, and gaps in coverage.
>
> ...
> Viewing the OLGC's concern about revealing video surveillance coverage in a broader sense, it is not clear to me from the OLGC's representations or from viewing the tape that it identifies the extent of such coverage in the facility. The tape appears to cover a relatively small area of the casino premises for a relatively short period of time. It is a compilation of portions of tapes from various cameras, each of which therefore has been edited. This alters what a person would otherwise see and therefore reduces the ability of someone viewing the tape to draw accurate inferences about the level and kind of surveillance.
>
> …
> The OLGC's descriptions of both the kind of harms it seeks to prevent and the manner in which these harms could result are vague and general, and do not provide the kind of "detailed and convincing" evidence required to establish the application of section 14(1)(i) or (l). They do not specifically point to anything about the level and kind of surveillance at this casino that does not reflect what the public already know about surveillance systems in casinos. Detailed descriptions of the types of surveillance systems in use at casinos, the scope of coverage of cameras, the level of detail cameras can capture, the makes and models of cameras sold for use in casinos, and legislative standards for casino surveillance systems are posted on the Internet. The OLGC did not identify any specific aspect of the design, operation, or capabilities of the system that would be revealed by viewing the videotape that is not generally known to the public or easily ascertainable.

[21] I note that the OLGC in ON IPC's Order PO-2358 discusses OLGC's concerns about the level and kinds of surveillance and not necessarily about the location of cameras, which is RPS' concern. However, similar to ON IPC's approach to reviewing the videos at issue and determining that the harm alleged by OLGC would be unlikely, it is not apparent that the disclosure of the eight videos would result in the harm alleged by the RPS. The RPS asserts that the disclosure of the videos could reveal which areas of the RPS headquarters are monitored and which areas aren't. I agree that disclosing the eight videos filmed by the one camera in the lobby would reveal the general location of the one camera that filmed the eight videos and the extent of the lobby that the camera films. However, it does not

reveal what other areas of the RPS headquarters are monitored, nor does it reveal if cameras pan or are fixed. Also, the disclosure of the eight videos would not reveal if there are additional cameras installed in the lobby of the headquarters. It just so happened that it was the one camera that captured the incident involving the Applicant. There could be other cameras that film other parts of the lobby but did not capture the incident involving the Applicant. Or there may not be other cameras. The disclosure of the eight videos simply would not reveal such information to the Applicant.

[22] Further, I acknowledge that the Applicant would have some knowledge of at least some of the layout of the RPS headquarters since they went undetected for a length of time before they were ultimately arrested in the lobby. However, disclosing the eight videos filmed by the one camera in the lobby would only inform the Applicant that there is indeed at least one camera in the lobby. If anything, it would deter the Applicant from breaking into the lobby of the RPS headquarters in the future. But it does not reveal what other parts of the RPS headquarters are monitored by surveillance cameras and which parts are not.

[23] I would also imagine RPS' security arrangements of its headquarters are not static in time. That is, if the Applicant was indeed able to break and enter into RPS' headquarters and had gone undetected for a length of time, that RPS would have taken action to prevent a similar incident from occurring in the future. That is, through this incident, RPS may have learned it had blind spots in its surveillance of its headquarters and could have improved its surveillance since then. The entirety of RPS' security arrangements of its headquarters is not solely dependent on the one camera in the lobby that captured the incident involving the Applicant.

[24] I find that that the first question is not answered in the affirmative. That is, RPS has not demonstrated that the disclosure of the eight videos of the lobby would reveal the security arrangements of RPS headquarters.

2. Could the release of information reveal security methods employed to protect particular vehicles, buildings, other structures, or systems?

[25] Earlier, I defined the terms “reveal”, “security”, “other structures or systems” and “could”.

[26] Page 91 defines the term “method” as a mode of organizing, operating, or performing something.

[27] In its submission, RPS said:

> - It is the position of the Regina Police Service that providing access to the videos requested by [Name of Applicant] would reveal security methods of the main lobby of the Regina Police Headquarters.
> - A security method refers to the specific approach or technique used to achieve security objectives. This can include principles, procedures, or tactics used to protect assets, information or individuals.
>   - Physical Security
>   - Technical Security
>   - Administrative Security
>   - Preventative Security
> - For the situation, involving [Name of Applicant] the security method RPS is considering is the Physical Security of our building. This method involves concrete measures to protect physical assets and the premise and our alarm systems and security cameras do this.
>
> As set out above, there are very significant concerns about the knowledge [Name of Applicant] was able to gain during his time unsupervised in the building. He knows the areas he broke into, and where items of interest are stored. Based upon this, he would be able to determine the physical location of a camera based upon the angle of the video. Confirming these locations will meet the second part of the security test, annunciated above.

[28] As noted earlier, RPS had indicated there is signage to notify the public that there are cameras on-sight. Therefore, through signage, RPS itself has disclosed its security method of using surveillance cameras to protect its headquarters.

[29] While the disclosure of the eight videos to the Applicant would reveal the general area in which one camera is located, it does not reveal other areas in which cameras are located. Nor would it reveal how the cameras are organized, operated, or utilized.

[30] I find that the second question is not answered in the affirmative.

[31] I find that RPS has not properly applied subsection 14(1)(m) of LA FOIP to the eight videos of the lobby.

[32] Since the eight videos of the lobby contain images of only the Applicant and RPS officers (and no third party individuals), then I recommend that the RPS release the eight videos, in full, to the Applicant within 30 days of issuance of the Report.

IV FINDING

[33] I find that RPS has not properly applied subsection 14(1)(m) to the eight videos of the lobby.

V RECOMMENDATION

[34] I recommend that RPS release the eight videos of the lobby to the Applicant within 30 days of issuance of this Report.

Dated at Regina, in the Province of Saskatchewan, this 15th day of October, 2024.

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