OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report A-2025-035

August 27, 2025

Department of Justice and Public Safety

Summary: The Complainant made an access request to the Department of Justice and Public Safety for video surveillance of themself from the St. John's Lock-Up. The Department responded to the request to deny access under section 31(1)(l) (reveal arrangements for the security of property) and section 40 (disclosure harmful to personal privacy). The Department also advised it was withholding access to the videos in their entirety as it did not have the means to redact the video. The Commissioner recommended the Department acquire the means to redact video records and to release the records subject to information-level exceptions under sections 31 and 40.

Statutes Cited: Access to Information and Protection of Privacy Act, 2015, SNL 2015, c A-1.2, sections 2, 8, 31, and 40.

Authorities Relied On: NL OIPC Reports A-2018-005 and A-2021-014.

OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador (June 26, 2015)

OIPC Guidance: Use of Video Surveillance (March 4, 2025)

BACKGROUND

[1] The Complainant made an access to information request to the Department of Justice and Public Safety under the **Access to Information and Protection of Privacy Act, 2015** (the "**Act**") for:

> All video of [Complainant] and or related to the [Complainant] matter inside and outside City of St. John's lockup from [Date], until [their] departure on [Date].

[2] The Department responded to the Complainant to advise it had searched for records but had made the decision to withhold all records pursuant to sections 40 (disclosure harmful to personal privacy) and section 31 (disclosure harmful to law enforcement). With respect to section 40, the Department advised: "The videos contain several third parties, and without appropriate redaction software, we are unable to release them due to privacy concerns" and with respect to section 31(1)(l) that: "the videos could disclose the locations and details of security cameras and related infrastructure at the St. John's Lockup."

[3] Following receipt of the Department's final decision, the Complainant made a complaint to this Office. As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 44(4) of the Act.

PUBLIC BODY'S POSITION

[4] In its submissions to this Office, the Department provided five videos from different cameras located inside and outside of the St. john's Lockup, all of which depict the Complainant and several other individuals. The Department notes the responsive videos contain footage of third parties and that images of individuals and characteristics that have the potential to be identifiable are protected as personal information. The Department also submits that disclosure of the responsive videos could disclose the locations and details of security cameras and related infrastructure at the St. John's Lockup and this could reasonably be expected to interfere with public safety.

[5] With respect to its application of sections 40 and 31, the Department submits that it does not have the software required to blur images or otherwise redact personal information or information that could reveal arrangements for the security of the St. John's Lockup. The Department further submits it is not subject to any legislative requirement to obtain the necessary software to process and disclose video records.

ISSUES

[6] This report will address the Department's applications of sections 31(1)(l) and 40, and its position that it is not required to acquire the tools to redact or sever information from video records.

DECISION

[7] Section 2 of the Act defines a "record" as "information in any form, and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner." It is clear that video recorded from a surveillance camera is a record. Section 8 of the Act further provides that an applicant has a right of access to any record in the custody or control of a public body, subject to any exceptions to access to information that can reasonably be severed from the record.

[8] While the exceptions to access relied on by the Department will be discussed in greater detail below, I will note as a preliminary matter that both section 31 and section 40 are "information-level" exceptions to access, as opposed to "record-level" exceptions. This means that only specific information can be withheld and the presence of personal information, or information that would reveal the arrangements for the security of a property or system, in a record does not necessarily, on its own, allow a public body to withhold the entire record. Instead, pursuant to section 8(2), an applicant is entitled to receive the remainder of a record after exceptions to access have been applied, if it is reasonable to sever the information from the record.

[9] This Office has previously addressed access to video records, most notably in A-2021-014, with the Office of the High Sheriff (a division of the Department of Justice and Public Safety). In that report, we recommended the Office of the High Sheriff obtain the necessary means to redact its video records and release records to the complainant. The Office of the High Sheriff agreed to follow those recommendations.

[10] Prior to A-2021-014, in 2018 we recommended the Town of Paradise "acquire or source the capacity to de-identify persons recorded by its surveillance cameras" (A-2018-005). And ten years ago, our 2015 OIPC Guidelines for Video Surveillance by Public Bodies advised public bodies that individuals whose personal information has been collected by surveillance cameras have a right to request their personal information and public bodies must have the means to accommodate such requests. These guidelines have since been updated in March of this year (OIPC Guidance: Use of Video Surveillance) with the same advice that organizations should develop policies and procedures for "how access requests for personal information will be handled, including technology to blur or block other identified individuals in the recording" and to "[a]cquire or source the capacity to de-identify (blur or block the identities of others) video surveillance records, which is an essential tool to process requests for access to records."

Section 31

[11] Section 31(1)(l) states:

> **Disclosure harmful to law enforcement**
>
> 31. (1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to
>
> . . .
>
> (l) reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;

[12] This is a discretionary, information-level exception. The test is whether it can be shown that disclosure could reasonably be expected to reveal arrangements for the security of a property.

[13] The Department's concerns around section 31 appear to be two-fold: one, the disclosure of the videos will disclose the very fact that surveillance cameras are used, the locations of those cameras, and what they are able to see; two, the video may contain further details of security at the St. John's Lockup.

[14] To assess the Department's application of section 31, this Office conducted a site visit of the St. John's Lockup pursuant to my powers under section 98 (right of entry). The St. John's Lock up is secured through a combination of various means, including physical security, video surveillance, and the use of procedures and practices. The presence of video surveillance is disclosed to the public on the exterior of the Lockup through signage and the exterior cameras are also visible to any passerby. The interior of the St. John's Lockup is not accessible to the general public and access is restricted. However, inside the Lockup, there is signage disclosing the presence of surveillance cameras and the interior cameras are also visible to the naked eye. I disagree that disclosing video recordings to the Complainant will disclose the mere fact that video surveillance is used in securing the St. John's Lockup.

[15] A further consideration may be whether disclosure will disclose the extent of the video surveillance and the details of camera sightlines that would reveal blind spots or locations not covered by video surveillance.

[16] As noted above, the Department disclosed five videos to this Office which it considered responsive to the Complainant's request. These videos, from five different surveillance cameras, represent only a small fraction of the cameras in use at the St. John's Lockup. Further, concerns about disclosing sightlines or blind spots could be addressed by using video redaction software to edit video imagery captured by any particular camera, while allowing the personal information of the Complainant to be disclosed.

[17] Finally, it is possible the videos could disclose details of other security arrangements such as, for example, physical security on doors or windows. As noted above, section 31(1)(l) is an information-level exception. Just as a document would be redacted to remove words or sentences subject to an exception, the Department may similarly redact or blur elements in a video that are also subject to an exception without denying access to the entire video.

Section 40

[18] Section 40 requires a public body to withhold personal information and it is a mandatory exception to access. This exception to access is subject to several provisions at section 40(4) which presume the disclosure of personal information in certain circumstances to be an unreasonable invasion of privacy. This presumption can be rebutted with reference to section 40(5). Conversely, it also deems at section 40(2) the disclosure of personal information in other circumstances to not be an unreasonable invasion of privacy.

[19] The records in question contain video of the Complainant interacting with several corrections officers and members of the Royal Newfoundland Constabulary. Some third parties who might be employees of the Department are also depicted in the videos. The videos do not contain audio.

[20] In its submission, the Department correctly notes that an individual's image is personal information, and that disclosure of their image may be an unreasonable invasion of privacy. This expectation of privacy exists even when the individual in question is a public employee. While section 40(2)(f), for example, allows the disclosure of some personal information about employees of public bodies, this does not necessarily extend to their image, which is a more sensitive form of personal information. We therefore agree there is a presumption that the disclosure of images of public body employees would be an unreasonable invasion of their privacy. In line with our conclusions in Report A-2021-014, the presumption is not rebutted: the videos provided to us for our review do not depict any actions by employees of the Department or of the Royal Newfoundland Constabulary that are clearly desirable to disclose for the purpose of public scrutiny. Further, the videos are not necessary for a fair determination of the Complainant's rights as a complaint about the conduct of any employee could be made in the absence of the videos.

[21] Having reviewed the videos and considered the application of section 40, I conclude it would be appropriate for the Department to release the videos with the faces of any third parties blurred. For civilian third parties, this will be sufficient to de-identify them. For corrections officers and Royal Newfoundland Constabulary officers, their uniforms provide

further anonymity while there is some benefit in being able to identify who is a uniformed officer discharging their duties.

Conclusions

[22] Video images collected by a public body through a surveillance camera is a record subject to the Act. Such surveillance cameras are increasingly ubiquitous in modern society and through this technology public bodies have the capacity to collect massive volumes of records, frequently collecting the personal information of third parties captured in the video. The Act does contemplate at sections 8(2) and 20(2) that there may be circumstances where a record cannot be provided; however, we cannot accept a blanket application of these circumstances to an entire class of record (video recordings) when the means exist to properly redact them and make them available. It is untenable for a public body to assert the right to generate these records, and collect personal information in this way, but not at the same time have any means of making the records available through the access to information process. Four years ago, following Report A-2021-014, the Office of the High Sheriff agreed to follow my predecessor's recommendations. It is disappointing to learn the Department responsible for the Office of the High Sheriff has still not obtained the means of processing its video records in compliance with the Act.

RECOMMENDATIONS

[23] Under the authority of section 47 of the **Access to Information and Protection of Privacy Act, 2015**, I recommend the Department of Justice and Public Safety, within 15 business days of today's date:

1. Acquire the capacity to de-identify persons or otherwise obscure video records, and
2. Release the videos to the Complainant subject to:
    a. Blurring the faces of any third parties, and
    b. Redacting any information within the videos subject to section 31(1)(l).

[24] As set out in section 49(1)(b) of the **Access to Information and Protection of Privacy Act, 2015**, the head of the Department of Justice and Public Safety must give written notice of his

or her decision with respect to these recommendations to the Commissioner and any person who was sent a copy of this Report within 10 business days of receiving this Report.

[25] Dated at St. John's, in the Province of Newfoundland and Labrador, this 27th day of August, 2025.

Kerry Hatfield
Information and Privacy Commissioner
Newfoundland and Labrador