OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report A-2021-014

March 1, 2021

Sheriff's Office

Summary: The Office of the High Sheriff (the "Sheriff's Office") received an access to information request for surveillance video recordings from the Supreme Court on Duckworth Street during a specified date at three different times and locations. The Sheriff's Office refused the request citing section 40 of the *Access to Information and Protection of Privacy Act, 2015* (disclosure harmful to personal privacy). Additionally, the Sheriff's Office contended that it did not possess the necessary equipment or software to de-identify the footage. The Commissioner concluded that the Sheriff's Office must acquire or source the capacity to de-identify persons recorded by its video surveillance systems. The Commissioner recommended that some video recordings be disclosed after they are de-identified. One video should be withheld in its entirety in accordance with section 40 because, under the circumstances, the identity of the individual may be known or reasonably ascertained despite any de-identification efforts.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, SNL 2015, c. A-1.2, ss. 2, 8, 20, and 40.

Authorities Relied On: NL OIPC Reports A-2019-009, A-2018-005; *OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador*; BC Order F15-42.

File # 0010-078-20-002

I BACKGROUND

[1] The Complainant made an access to information request under the *Access to Information and Protection of Privacy Act, 2015*, ("*ATIPPA, 2015*" or the "*Act*") to the Office of the High Sheriff (the "Sheriff's Office") for videos related to the Supreme Court House on Duckworth Street on September 18, 2020, as follows:

- Footage from the main sidewalk/front entrance (between 9:30 and 10:00am);
- Footage from the staff-only entrance where he alleges an individual was allowed to exit circumventing the Complainant's ability to confront the individual (from 9:30 - 10:30am); and
- Footage from inside the main building showing that officers made him leave but allowed another individual to stay (from 9:40 - 10:00am).

[2] The Sheriff's Office refused to provide the Complainant with the requested records, citing section 40 (disclosure harmful to personal privacy) and section 20 (provision of information).

[3] The Complainant filed a complaint with this Office. As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 44(4) of *ATIPPA, 2015*.

II PUBLIC BODY'S POSITION

[4] The Sheriff's Office denied access to the requested records in accordance with section 40, citing unreasonable invasion of a third party's personal privacy. The Sheriff's Office indicated that a review of the responsive records determined that the video contained personal information of individuals other than Sheriff's Officers or the Complainant. It submitted that it does not have the software required to blur images in video, and such technology is not within its normal computer hardware and software technical expertise. The Sheriff's Office also noted that for some of the videos, the Complainant had indicated he knew one of the individuals who would be in the video and, therefore, even if the videos could be blurred, this would not protect the privacy of the individual in question.

[5] In an additional submission to this Office, the Sheriff's Office explained:

> *The lack of software is not the reason for citing section 40. The reason for citing section 40 is that the disclosure of the videos in their current state would be an unreasonable invasion of privacy. The lack of software, is the reason that the videos cannot be released, as the Sheriff's Office does not have the capability to make the appropriate, mandatory redactions to the videos.*

[6] The Sheriff's Office also argued that it does not have the resources or expertise required to process such a request, even in the event that it did have the software to do so:

> *To blur out each image requires a frame by frame review of the videos and the appropriate application of redactions. Depending on the video used, each frame could have 13-25 frames per second of video. Only a few minutes of the videos constitute the applicant's personal information, however, they consist of four hours and eight minutes of footage. Many of the videos include multiple individuals, some of whom have distinctive characteristics, which would require redactions in addition to general facial redactions to ensure de-identification. This would require the Office to review between 193,440 and 372,000 frames of footage. To do so would unreasonably interfere with the operations of the Office.*

[7] The Sheriff's Office therefore proposed an alternative option to disclosure, arguing that the more appropriate solution to this complaint would be to allow the applicant to view the video recording of himself in person:

> *It is felt that allowing him to view the video, without providing a copy, would balance his right to his own personal information and the privacy of the individuals within the video, as he would not have a copy that could be used or disclosed afterwards.*

III COMPLAINANT'S POSITION

[8] The Complainant submitted that access to the records in question should be granted because he did not believe they contained any personal information of individuals. He submitted that the videos would only show a person's appearance and that those visible were in public spaces where no expectation of privacy exists.

[9] The Complainant also took exception to the Sheriff's Office's position that, because he knows the identity of one of the individuals in the videos, even if it were able to blur out that

individual it would be an unreasonable invasion of their privacy to disclose the videos to him. The Complainant stated, “the only 'private information' would be their faces which I already know who they are…there is NO private information available besides the faces of these officers and every single officer had to be sworn in.”

V DECISION

[10] Section 8 of *ATIPPA, 2015* states:

> *8. (1) A person who makes a request under section 11 has a right of access to a record in the custody or under the control of a public body, including a record containing personal information about the applicant.*
>
> *(2) The right of access to a record does not extend to information excepted from disclosure under this Act, but if it is reasonable to sever that information from the record, an applicant has a right of access to the remainder of the record.*

[11] While the Complainant has a clear right of access, particularly for records containing his personal information, this right does not extend to information excepted from disclosure pursuant to other provisions of *ATIPPA, 2015*.

Section 40 (disclosure harmful to personal privacy)

[12] The relevant portions of section 40 of *ATIPPA, 2015* are as follows:

> *40. (1) The head of a public body shall refuse to disclose personal information to an applicant where the disclosure would be an unreasonable invasion of a third party's personal privacy.*
>
> *(2) A disclosure of personal information is not an unreasonable invasion of a third party's personal privacy where*
>
> *(a) the applicant is the individual to whom the information relates;*
>
> *. . .*
>
> *(f) the information is about a third party's position, functions or remuneration as an officer, employee or member of a public body or as a member of a minister's staff;*

(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy where

(c) the personal information relates to employment or educational history;

(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body shall consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the province or a public body to public scrutiny;

(b) the disclosure is likely to promote public health and safety or the protection of the environment;

(c) the personal information is relevant to a fair determination of the applicant's rights;

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;

(e) the third party will be exposed unfairly to financial or other harm;

(f) the personal information has been supplied in confidence;

(g) the personal information is likely to be inaccurate or unreliable;

(h) the disclosure may unfairly damage the reputation of a person referred to in the record requested by the applicant;

(i) the personal information was originally provided to the applicant; and

(j) the information is about a deceased person and, if so, whether the length of time the person has been deceased indicates the disclosure is not an unreasonable invasion of the deceased person's personal privacy.

[13] The responsive records are five video recordings taken from different cameras in and around the Supreme Court of Newfoundland and Labrador Court House on Duckworth Street. The videos feature a number of individuals: the Complainant, Sheriff's Officers and various other third parties walking by the Court House, standing near the entrance, and exiting and entering the Court House. The Sheriff's Office argues that disclosing the video recordings would disclose personal information of those individuals.

[14] The Sheriff's Officers and the other third parties are identifiable persons. The depictions of these persons consist of personal information as defined in section 2(u) of the Act:

> *2(u)(ii) "personal information" means recorded information about an identifiable individual . . .*

[15] In keeping with this Office's analysis in Report A-2021-009, the videos contain personal information as defined under section 2(u) of *ATIPPA, 2015*, as it clearly captured recorded information about identifiable individuals other than the Complainant, including both third parties and Sheriff's Officers.

[16] The Complainant is entitled to receive all information that is not subject to an exception, meaning he is allowed to receive, unredacted, images of himself and images of any other individuals, either members of the public or Sheriff's Officers, where the disclosure of their personal information would not be an unreasonable invasion of their personal privacy. Disclosure of the images of other members of the public would normally constitute an unreasonable invasion of a third party's personal privacy pursuant to section 40(1), which is then subject to the balancing provision in section 40(5). Section 40(5) provides for a determination of whether the disclosure of personal information would be an unreasonable invasion of privacy through consideration of relevant circumstances, examples of which are listed in the provision.

[17] We will next address the personal information of the Sheriff's Officers that is captured in the video. At section 40(2), *ATIPPA, 2015* provides several scenarios where disclosure of personal information is deemed to not be an unreasonable invasion of an individual's personal privacy. One scenario, at section 40(2)(f), allows disclosure of information about a third party's position, functions or remuneration as an officer, employee or member of a public body. Conversely, disclosure of personal information related to employment history is presumed to be an unreasonable invasion of a third party's personal privacy under section 40(4)(c). The question then is whether images of the Sheriff's Officers fall under 40(2)(f) or 40(4)(c). The British Columbia Office of the Information and Privacy Commissioner, in Order F15-42, provides some guidance:

> *[35] I agree with Alberta Order F2008-020 that video footage about a topic will frequently contain more detailed personal information than written information because it captures information in the form of images and audio recordings (including tone, physical identity, non-verbal body language and cues, mannerisms, etc.). In the context of ss. 22(4)(e) and 22(3)(d) of FIPPA, the*

> *distinction between video and audio recordings compared to written records may be relevant. In my view, audio and video footage about an employee is more likely to be "about" that specific employee, their actions and how they do their job compared to a written record created in the course of an employee's ordinary functions, tasks and activities. This is due in large part to the additional amount of detail that is contained in video footage compared to written records. I find that this is the case here, and that the video footage is about the specific employees, not their ordinary job functions, tasks and activities.*

[18] If we find that the disclosure of personal information of the Sheriff's Officers is presumed to be an unreasonable invasion of their personal privacy under 40(4)(c), it may still be rebutted with reference to section 40(5). Several of the enumerated considerations at 40(5) may be relevant. In particular, section 40(5)(a) requires a public body to consider whether disclosure of the information is desirable for the purpose of subjecting the activities of the Sheriff's Office or its officers to public scrutiny. Further, section 40(5)(c) requires consideration of whether the information is relevant to a fair determination of the Complainant's rights.

[19] Sheriff's Officers are law enforcement officers tasked with providing court security, bailiff services, and enforcing judgments. Sheriff's Officers are authorized to arrest and detain individuals, and are responsible for pre-trial detention of accused persons. They interact with the public and such interactions may, at times, be physical. Given this, it may be desirable to disclose personal information in order to effectively scrutinize the activities of the Sheriff's Office where the circumstances require it. The Complainant suggested in his submission to this Office and in his original access to information request for the video that he was seeking it, at least in part, in relation to a specific interaction he had with Sheriff's Office staff in order to review the matter and have proof of the interaction. Depending on what, if anything, arises from such an interaction then there may be some consideration here to the applicability of sections 40(5)(a) and (c), in favouring disclosure. The footage would provide transparency of the incident and the ability to hold the public body and its staff accountable for any actions or inactions. Likewise, disclosure could be relevant to a fair interpretation of the Complainant's rights with respect to these encounters.

[20] Having reviewed the videos, it is not apparent to me that there were any specific actions by Sheriff's Officers that are desirable to disclose in order to expose the Sheriff's Office to

public scrutiny. Likewise, the Complainant has not made out how a copy of the video, with the identities of Sheriff's Officers disclosed, is relevant to a fair determination of his rights. If the Complainant wishes to make a complaint to the Sheriff's Office about the conduct of its officers, he is able to do so without first obtaining the video. If the Complainant believes he has a legal claim, then his cause of action would likely lie against the Sheriff's Office itself and, if the video is necessary for determining his rights, it can be provided during the document disclosure process. I am therefore satisfied that the personal information of the Sheriff's Officers should be withheld. However, in accomplishing this, I am of the view that it would be appropriate for the Sheriff's Office to redact only the faces of the Sheriff's Officers. The Sheriff's Officers' uniforms will provide sufficient anonymity once their faces are blurred and I believe there is still some residual benefit in being able to identify which individuals in the video are public employees discharging their duties.

[21] Finally, we need to consider the personal information of the third parties – that is, those members of the public who had business at the Court House that day, or were merely passing by on the sidewalk. As noted above, their images are their personal information and section 40(1) would require that that personal information be withheld, subject to consideration of any relevant circumstances at section 40(5). None of the considerations in section 40(5) appear to support disclosure of these images in identifiable form, which leads to the conclusion that unredacted disclosure of those images would be an unreasonable invasion of privacy in accordance with section 40(1). Once that conclusion is reached, the exception to access is mandatory.

[22] The Sheriff's Office argued that several of the individuals involved had "distinctive characteristics" such that even if it were to have the capacity to blur images it remained concerned that de-identification would not be possible. I am satisfied that using appropriate video redacting software, the Sheriff's Office can, and should, blur the entire bodies of any third parties present in the video. Once done, the likelihood of identifiability through "distinctive characteristics" would be low.

[23] With respect to one video, depicting the Court House staff-only entrance, the Sheriff's Office made the argument that the Complainant knows the identity of an individual in that

video and has a direct and adverse relationship with this person, so even were the Sheriff's Office to have the capacity to fully blur individuals, the Complainant would still be aware of this person's identity. Even utilizing the necessary technology to blur images, the ability to de-identify the individuals in this video is therefore limited.

[24] I accept that in this instance, even if the identity of the individual was blurred out, the video would still reveal information about the person in question as the Complainant is able to re-identify them. This would constitute an unreasonable invasion of the third party's personal privacy. Where a record contains the personal information of another person, the Complainant's right of access to his own personal information under section 40(2)(a) of *ATIPPA, 2015* is subject to, and must be balanced against, the protection of other individuals' personal information. In Report A-2021-009, I stated,

> *… there could be situations in which, as with the present situation, it was impossible to shield personal information from disclosure but in which disclosure could be considered to be a reasonable invasion of personal privacy if it is desirable for the purpose of subjecting the activities of a public body to scrutiny under section 40(5)(a).*

[25] As noted above, where a record contains personal information, determining whether its disclosure constitutes an unreasonable invasion of that third party's personal privacy is subject to consideration of all relevant circumstances, pursuant to section 40(5).

[26] With respect to this video, the Complainant identified frustration with not being able to confront the individual in the video. However, no evidence was provided that the ability to engage in such a confrontation is a lawful right that was denied to the Complainant. Nor is there evidence that disclosing personal information about this individual is desirable for the purpose of subjecting the activities of the Sheriff's Office to public scrutiny. Given the circumstances of the incidents, the acrimonious relationship of those involved and that the Complainant is aware of who the third party is, even fully blurred versions of these videos would reveal personal information. As the images are identifiable to the Complainant even if they were blurred, we must therefore treat those as identifiable. Therefore, it must be concluded that even disclosure of the blurred video would result in disclosure of personal information in this context, and nothing in section 40(5) would allow us to conclude that such a disclosure would not be an unreasonable invasion of privacy.

[27] The Complainant expressed the view that he should receive full access to the video recordings because there was no expectation of privacy in a public space. This is a misunderstanding of the applicable law. When access to information is requested from a public body in Newfoundland and Labrador, the provisions of *ATIPPA, 2015* are engaged. It is not as straightforward as the Complainant imagines. Furthermore, when it comes to these kinds of requests, it is worth reflecting on the fact that acquiring a copy of a video recording of someone is more privacy-sensitive than simply seeing them in-person. Once a video is obtained, it can be distributed, altered, or posted to social media, which can have significant and long-lasting impacts. Therefore, such disclosure must be done only in accordance with *ATIPPA, 2015* after due consideration of all relevant provisions, including the relevant circumstances in section 40(5), if applicable.

[28] The Sheriff's Office, in its final submission to this Office, suggested an alternative to disclosure: allowing the Complainant to view the video recording of himself in person as a way to balance his right to his own personal information and the privacy of the individuals within the video. However, the Complainant did not request to view the record but to obtain a copy. Furthermore, we do not see any legal distinction in the present case between allowing the Complainant to view the record and to obtain a copy of the record and any viewing would be subject to the same redactions I have outlined above.

[29] Given the foregoing analysis, we conclude that four of the videos can be disclosed to the Complainant, subject to the use of software to blur the faces and bodies of any third parties and the faces of any Sheriff's Officers who appear. However, the staff-only entrance video should continue to be withheld pursuant to section 40(1) of *ATIPPA, 2015*.

Section 20 – provision of information

[30] Relevant portions of section 20 state:

> *20. (1) Where the head of a public body informs an applicant under section 17 that access to a record or part of a record is granted, he or she shall*
>
> > *(a) give the applicant a copy of the record or part of it, where the applicant requested a copy and the record can reasonably be reproduced; or*

> *(b) permit the applicant to examine the record or part of it, where the applicant requested to examine a record or where the record cannot be reasonably reproduced.*
>
> *(2) Where the requested information is in electronic form in the custody or under the control of a public body, the head of the public body shall produce a record for the applicant where*
>
> *(a) it can be produced using the normal computer hardware and software and technical expertise of the public body; and*
>
> *(b) producing it would not interfere unreasonably with the operations of the public body.*

[31] The Sheriff's Office submitted that there is no legislative requirement to purchase appropriate software to blur images in CCTV footage to allow for disclosure. It also argued that in the absence of a clear legislative requirement, and in addition to sections 8(2) and 20(2) of *ATIPPA, 2015* which clearly contemplate circumstances in which documents will not be able to be produced for an applicant, it had met its obligations under the *Act*.

[32] In Report A-2018-005, this Office previously recommended the Town of Paradise, "acquire or source the capacity to de-identify persons recorded by its surveillance cameras," when the public body argued that its lack of such capacity constituted grounds for denying disclosure. Additionally, our guidance document, *OIPC Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador,* which was released in 2015, sets out essential considerations for public bodies when making a decision to decide whether or not to use CCTV, noting:

> *10. Are the rights of individuals to have access to their personal information respected?*
>
> *People whose images are recorded have a right under ATIPPA, 2015 to request access to their recorded personal information, including their image recorded by CCTV. Severing the personal information in a recording (including software to implement blurring or blocking of the identities of others) may be necessary to allow individual access. Policies and procedures must accommodate such requests.*

[33] The Department of Justice (the "Department") is aware of this guidance, and should have ensured that the various entities for which it is responsible, such as the Sheriff's Office, were following it. The means to de-identify surveillance video records is an essential part of any CCTV system operated by a public body, and if a public body implements CCTV capability it also needs redaction software, as it is an essential tool required to process requests for access to records. If you have paper records, you need a black marker; if you have electronic records (including video surveillance records), you need electronic redaction software. In our review of decisions from other jurisdictions, it is clear that other public bodies are using redaction software to sever personal information from video surveillance records. A cursory internet search reveals numerous software programs are available, many of them specifically marketed to law enforcement.

[34] I therefore do not find merit in the Sheriff's Office's argument that it is relieved of its obligation to fulfill this access to information request because it has failed to acquire the appropriate software. The Department and its affiliate entities, of which the Sheriff's Office is one, are sophisticated public bodies with resources and staffing certainly surpassing many municipal public bodies in this province that are able to process requests in this manner. Redaction software for CCTV is basic and easily accessible. In many cases, the process is highly automated and does not require the frame-by-frame process described by the Sheriff's Office in its submissions. Failure to acquire what would otherwise be considered the "normal hardware and software" is not a free ticket to avoid fulfilling access to information requests of this nature.

[35] I likewise do not find compelling the Sheriff's Office argument that to utilize redaction software would, in this or any other case, constitute an unreasonable interference with its operations. In the specific matter at hand, the total running time of all five videos is less than two hours. However, even if the request had been for a much larger CCTV record, the Sheriff's Office had the ability, as it does with any access request it believes it cannot complete within the legislative time frame, to seek an extension from this Office.

[36] While I will be recommending that the Sheriff's Office or the Department obtain the ability to redact video records and appropriately redact the responsive records, I recognize that the Sheriff's Office position is that they do not presently have this ability. As such, I believe it is appropriate to afford the Sheriff's Office 20 business days following its receipt of this report to provide responsive records to the Complainant, as if it were processing an access to information request anew.

VI RECOMMENDATIONS

[37] Under the authority of section 47 of the *ATIPPA, 2015*, I recommend that the staff-only entrance video continue to be withheld from the Complainant in accordance with section 40. For the other four videos, I recommend that the head of the Office of the High Sheriff, within 20 business days of today's date, acquire the capacity to de-identify persons recorded by its CCTV surveillance cameras, de-identify any third parties other than the Complainant and Sheriff's Office staff, blur the faces of the Sheriff's Officers, and disclose the remainder to the Complainant.

[38] As set out in section 49(1)(b) of *ATIPPA, 2015*, the head of the Office of the Sheriff 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.

[39] Dated at St. John's, in the Province of Newfoundland and Labrador, this 1st day of March 2021.

Michael Harvey
Information and Privacy Commissioner
Newfoundland and Labrador