OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2016-001

May 2, 2016

Department of Justice and Public Safety

Summary: The Complainant submitted three privacy complaints against the Department of Justice, now known as the Department of Justice and Public Safety (the "Department") under the *Access to Information and Protection of Privacy Act* (the "*ATIPPA*"). Two of the complaints involved the use of audio and video surveillance systems at the St. John's Lockup and the third complaint involved the disclosure of personal information. The first complaint was resolved and the Commissioner made a recommendation that the Department adopt policies and procedures related to its surveillance practices. This Office then attempted to follow up on the implementation of this recommendation and no indication of compliance was forthcoming. In respect of the remaining complaints the Department did not respond in a timely or sufficient manner. Given the related issue of excessive delays and the possibility of a systemic problem, the Commissioner decided to respond to all three matters collectively. The Commissioner found that Department failed to comply with the recommendations in respect of the first complaint; the Department used the Complainant's personal information contrary to the *ATIPPA* in respect of the second complaint; and improperly disclosed and inadequately protected the Complainant's personal information in respect of the third complaint. The Commissioner made several recommendations to the Department relating to both its need for policies and procedures and the need for more timely and diligent actions by the Department when responding to this Office.

Statutes Cited: *Access to Information and Protection of Privacy Act*, S.N.L. 2002, c. A–1.1, as amended, ss. 32, 36, 38, and 39; *Access to Information and Protection of Privacy Act, 2015*, S.N.L. 2015, c. A-1.2, s. 64

Authorities Relied On: *Protection of Privacy, Policy and Procedures Manual,* November 2015. Government of Newfoundland and Labrador, ATIPP Office, Office of Public Engagement

BACKGROUND

Incident 1

[1] On May 1, 2013, this Office received a Privacy Complaint in relation to the use of motion-activated audio recording systems in selected areas of the St. John's Lockup. The matter was reviewed by this Office and it was determined that there was a rational basis for these security measures, and that they were directly related to and necessary for the safe operation of the Lockup. As such, I concluded that the use of the cameras and their audio feature, including their motion activated nature, is not a breach of section 32 of the *ATIPPA.* I was also satisfied that the Department had taken appropriate measures to ensure that the surveillance cameras were used in a minimally privacy intrusive manner.

[2] However, I requested that the Department adopt comprehensive policies and procedures (to be reviewed and updated as necessary) to direct practices related to the video surveillance system, as none existed at that time. I indicated that these policies and procedures should be in writing and include the following:

- the rationale and purpose of the system;
- system guidelines that include: the location and field of vision of equipment, list of authorized personnel to operate the system, when surveillance will be in effect, and whether and when recordings will be made;
- notice of use of surveillance, providing access, use, disclosure, security, retention and destruction of records;
- the responsibilities of all service providers (employees and contractors) to review and comply with policy and statute in performing their duties and functions related to the operation of the video surveillance system;
- the consequences of breach of contract or policy.

[3] In December, 2013 I advised the Department that my Office would be in contact in three months to follow up on the progress of these policies. This follow up occurred on April 17, 2014 and no response was received. However, the matter was discussed in a response provided in relation to Incident 2 and Incident 3 dated October 22, 2015.

Incident 2

[4] On December 29, 2014, this Office received another Privacy Complaint from the same individual also relating to audio and video recording systems at the St. John's Lockup. In this instance the matter was specific to a human resources investigation. Follow-up in relation to Incident 1 in regards to policies and procedures was brought under the umbrella of this matter.

[5] The Department did not respond until March 6, 2015 and the response was brief and lacking in detail. Consequently, this Office requested further information from the Department including a written response outlining the Department's policy position on the use of the audio recordings in the specific circumstances.

[6] The Department did not respond to this request despite reminders from this Office. On June 25, 2015, I wrote the Deputy Minister in an effort to move this matter forward. A response was received from the Department on October 22, 2015. While this response did address some of the issues raised in this matter, it did not address the outstanding issue in respect of the Department's lack of policies and procedures related to the audio/video surveillance system.

Incident 3

[7] On December 29, 2014, this Office received another Privacy Complaint from the same individual regarding a breach that occurred on December 18, 2014 when the contents of a protected drive were inadvertently copied to a common drive and thereby became accessible by many employees.

[8] The Department did not respond until March 6, 2015 and the response did not contain all of the information we were seeking. Consequently, this Office requested further information from the Department regarding the notification process that was carried out for those affected by the breach.

[9] The Department did not respond to this request for quite some time despite reminders and follow-up from this Office. From conversations with the Department's Coordinator, it appeared that the Department was considering the method of notification. On June 25, 2015, I wrote the Deputy Minister in an effort to move this matter forward. A response was finally received from the

Department on August 24, 2015 consisting solely of a copy of the mass notification sent to all staff regarding the breach. This notice was sent out almost 9 months after the original privacy breach occurred. Also, as noted in a letter from my Office on August 27, 2015, the notice was incomplete as it did not include the contact information for this Office such that employees would be aware of their right to file a complaint. A revised notice was issued September 14, 2015.

[10] The delays and lack of a timely response by the Department are concerning and disheartening. The ability of this Office to discharge its mandate in respect of privacy complaints is not merely hindered where a public body chooses not to actively participate in the processes of this Office, it is entirely frozen. The only action which remains is to proceed to a public Report. However, that process is also hindered as this Office is often left with no real interactions or discussions with the Department on which to form a substantive decision.

[11] I have decided to provide a written Report on all three of these matters collectively in order to address this concern while also attempting to resolve the outstanding issues in these matters.

II PUBLIC BODY'S SUBMISSION

[12] The only substantial representation put forward by the Department since the closure of Incident 1 was submitted on October 22, 2015.

[13] In respect of Incident 2, the Department acknowledged the use of the audio and video surveillance systems for a human resources investigation. The Department indicated that at the time of the incident the St. John's Lockup was undergoing a 'Proof of Concept" ("POC") for an upgraded audio/video surveillance system which included three (3) cameras.

[14] The Department pointed out that the audio capabilities of this system were reviewed by this Office in relation to Incident 1 in 2013 and, as stated at that time, one of the responsibilities of the Adult Corrections Branch of the Department is to maintain safe and secure correctional facilities.

[15] The Department also pointed out that in relation to Incident 1, this Office accepted that the use of audio and video systems at the St. John's Lockup was permissible in accordance with section 32 of the *ATIPPA* as it related directly to and is necessary for an operating program or activity of the public body. The Department maintained that this position was still applicable and the use of the cameras and audio were consistent with the objectives of safety and security.

[16] The Department indicated that the POC was in operation for two years, since approximately 2013, and was being upgraded starting in August 2015. The Department indicated that no new capabilities would be installed until an approved policy on video and audio surveillance was completed.

[17] No additional information or policies in respect of video and audio surveillance at the St. John's Lockup has been provided to date, despite the previous repeated attempts to obtain same in relation to Incident 1 and its follow-up.

III DISCUSSION

[18] Each matter presents its own set of issues along with the shared issue of excessive delays.

Incident 1

[19] The issue remains the lack of policies and procedures as requested at the conclusion of this matter.

[20] The Department has not at any time since the conclusion of this matter provided the information as requested by this Office. The Department, to the best of my knowledge, has not created any policies and procedures to govern its use of video and audio surveillance systems within the St. John's Lockup.

Incident 2

Was the Complainant's personal information collected in a manner which is authorized by section 32 of the *ATIPPA*?

[21] Section 32 of the *ATIPPA* states:

32. No personal information may be collected by or for a public body unless

(a) the collection of that information is expressly authorized by or under an Act;
(b) that information is collected for the purposes of law enforcement; or
(c) that information relates directly to and is necessary for an operating program or activity of the public body.

[22] In a previous examination of the use of video and audio surveillance systems in the St. John's Lockup this Office indicated that the use of video and audio surveillance systems at the St. John's Lockup is necessary and was not contrary to section 32 as the collection is related directly to and was necessary for an operating program or activity of the public body.

[23] Without being provided with policies and procedures in this regard, I must assume that the purpose for which the information is collected is still that which is outlined in the Department's submission: to maintain the safety and security of correctional facilities for inmates, staff and members of the public. Therefore, as the rationale for the collection remains the same, I reiterate the above decision.

Was the Complainant's personal information used in a manner which is authorized by section 38 of the *ATIPPA?*

[24] Section 38 of the *ATIPPA* states:

38. (1) A public body may use personal information only

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 40 ;
(b) where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or
(c) for a purpose for which that information may be disclosed to that public body under sections 39 to 42 .

(2) The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.

[25] In this instance, the personal information which was collected was used for the purpose of a human resources investigation; to determine if an employee disobeyed a direct order. I do not accept that this use is for the "*purpose for which that information was obtained or compiled".* Similarly, I do not believe that this use was for a consistent purpose as described in section 40 as, without policies and procedures in place, I am unable to state with certainty that the use had a reasonable and direct connection to the need for safety and security.

Incident 3

Was the Complainant's personal information disclosed in a manner which is authorized by section 39 of the *ATIPPA?*

[26] The Department has identified this incident as a privacy breach. It acknowledges that the Complainant's personal information, and that of others, was accidentally inappropriately released and available to a number of employees for a limited amount of time.

[27] I accept the Department's categorization of this incident as a breach, as there is no basis under section 39 for the disclosure of the information in the manner that occurred.

Was the Complainant's personal information protected in accordance with section 36 of the *ATIPPA?*

[28] Section 36 of the *ATIPPA* states:

> *36. The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal*

[29] While I appreciate that this incident occurred simply as the result of human error, I am not satisfied that the Department has adequate security arrangements in place to protect against disclosures such as these.

[30] Administratively, the Department has taken reasonable steps to protect personal information, including reminding employees of their obligations and best practices for handling employee information and making employees aware of policies regarding the use of electronic files via standing orders and OCIO directives.

[31] However, in regard to physical and technological safeguards, I do not believe the Department has taken reasonable steps. The Department has not indicated that it has evaluated or implemented any such safeguards in relation to personal information held on employee computers and the use of such information. Enhanced access controls are simply one step which the Department could take to better protect personal information.

Were the affected individuals properly notified of this incident?

[32] I appreciate that at the time this breach occurred mandatory breach notification was not part of the *ATIPPA* which was in force then. However, due to the delays experienced on this matter I believe it is practical for the Department to now turn its mind to its obligations under the current *Act*.

[33] In relation to the notification of affected individuals, section 64 of the *ATIPPA, 2015* states:

> *64* [...] *(3) Except as otherwise provided in subsections (6) and (7), the head of a public body that has custody or control of personal information shall notify the individual who is the subject of the information at the first reasonable opportunity where the information is*
>
> *(a) stolen;*
> *(b) lost;*
> *(c) disposed of, except as permitted by law; or*
> *(d) disclosed to or accessed by an unauthorized person.* [...]
>
> *(6) Where a public body has received personal information from another public body for the purpose of research, the researcher may not notify an individual who is the subject of the information that the information has been stolen, lost, disposed of in an unauthorized manner or disclosed to or accessed by an unauthorized person unless the public body that provided the information to the researcher first obtains that individual's consent to contact by the researcher and informs the researcher that the individual has given consent.*
>
> *(7) Subsection (3) does not apply where the head of the public body reasonably believes that the theft, loss, unauthorized disposition, or improper disclosure or access of personal information does not create a risk of significant harm to the individual who is the subject of the information.*
>
> *(8) For the purpose of this section, "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or*

professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property.

(9) The factors that are relevant to determining under subsection (7) whether a breach creates a risk of significant harm to an individual include

(a) the sensitivity of the personal information; and
(b) the probability that the personal information has been, is being, or will be misused.

[34] The decision to notify and the process to be taken in this matter took over eight months. I note that in March, 2015 the Department indicated it was in the process of preparing notifications. Consequently, a decision had been made at that time to notify and I can see no justification for the further delay of five (5) months.

[35] I remind the Department of the *Protection of Privacy, Policy and Procedures Manual,* November 2015 produced by the ATIPP Office of the Office of Public Engagement wherein it states:

<u>When and How to Notify</u>
When to Notify: Subsection 64(3) requires that individuals be notified (where required) ***at the first reasonable opportunity****. Notification of affected individuals should occur as soon as possible following the breach. However, if you have contacted law enforcement officials, you should determine from those officials if you should delay notification so as not to impede a criminal investigation.*
How to Notify: The preferred method of notification is direct notification. Direct notification may be via a phone call, a letter or in person. Indirect notification, such as website information, posted notices or media, should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is unavailable. In certain cases, using multiple methods of notification may be the most effective approach.

<u>Information to be Included in the Notification</u>
Notifications should include the following pieces of information:
- *date of the breach;*
- *description of the breach;*
- *description of the information inappropriately accessed, collected, used or disclosed;*
- *steps taken so far to mitigate the harm;*

> • *next steps planned and any long term plans to prevent future breaches;*
>
> • *steps the individual can take to further mitigate the risk of harm;*
> • *contact information of an individual within the public body or organization who can answer questions or provide further information; and*
>
> • *contact information for the Office of the Information and Privacy Commissioner, to whom individuals have the right to file a complaint regarding a breach of privacy.*
>
> *The information should be general and should not include the personal information that was breached. For example, you can say that the individual's date of birth was inappropriately disclosed, but you would not state the individual's actual date of birth in the notification*.
>
> [Emphasis added]

IV CONCLUSION

Incident 1

[36] The Department has failed to comply with the recommendations issued in this matter.

Incident 2

[37] The Complainant's personal information was collected in a manner which is authorized by section 32 of the *ATIPPA,* as the collection is related directly to and is necessary for an operating program or activity of the public body.

[38] However, without policies and procedures from the Department I am unable to conclude that the Complainant's personal information was used in a manner which is authorized by section 38 of the *ATIPPA*. For the same reason, I am also unable to conclude that the disclosure of the Complainant's personal information was in accordance with section 39.

Incident 3

[39] The Complainant's personal information was disclosed in a manner which was not authorized by section 39 of the *ATIPPA.*

[40] The Complainant's personal information was not adequately protected in accordance with section 36 of the *ATIPPA.*

[41] Notification of the breach was not required under the legislation in place at the time of the incident; however, the Department had indicated that it was prepared to notify and in my opinion a timeframe of eight months was undue for this particular circumstance. This is especially so given the notification requirements under the new *Act* which came into force on June 30, 2015. While the new *Act* did not apply to this particular complaint, I would have expected that procedural changes associated with the coming into force of the new *Act* would have resulted in this matter being dealt with more expeditiously.

V RECOMMENDATIONS

[42] The Department's continuous non-cooperation with this Office is troubling. This is not the first time the Department failed to communicate in a timely manner with this Office. This Office has been more than accepting and lenient with the Department in this regard; however, should such actions continue to occur I remind the Department that the time lines, expectations and legal processes under the *ATIPPA, 2015* do not allow for this type of response.

[43] In light of the foregoing, it is my recommendation that the Department take immediate steps to:

i. develop and implement detailed policies and procedures in respect of all video and audio surveillance systems at the St. John's Lockup;
ii. implement appropriate measures to safeguard personal information; and
iii. develop, post and provide appropriate training to all employees regarding the collection, use and disclosure of personal information

[44] The Department should endeavor to have these tasks completed within 60 days of receiving this Report, and this Office will initiate follow-up with the Department to ensure these obligations are fulfilled.

[45] In recent months the Department has had several reminders from this Office on its lack of responsiveness and participation in a number of files in addition to those discussed herein. Although I acknowledge the Department's performance has improved somewhat, it is not where

this Office would expect it to be. Consequently, it is also my recommendation that the Department take steps to:

iv. be more diligent and timely in its approach to fulfilling its duties and obligations under the *ATIPPA, 2015*;
v. make a greater effort to communicate in a timely manner with this Office;
vi. review its policies and procedures for notifying affected individuals of privacy breaches and
vii. review its policies and procedures for handling and responding to complaints from this Office.

[46] The Department is requested to please respond to these recommendations within 14 days of receiving this Report, indicating its response to each of the recommendations and the expected completion date for each.

[47] Dated at St. John's, in the Province of Newfoundland and Labrador, this 2nd day of May 2016.

E. P. Ring
Information and Privacy Commissioner
Newfoundland and Labrador