OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

P-2018-003

April 3, 2018

Town of Paradise

Summary: This Office received a complaint regarding the collection and use of personal information recorded by the Town's video surveillance system. The Town declined to provide much of the information requested during our investigation. Based on the available information the Commissioner determined that the Town's video surveillance system was collecting personal information without authorization as set out in the *ATIPPA, 2015*. The Commissioner recommended that the Town stop collecting personal information using the Town's video surveillance system until it can demonstrate to the satisfaction of the Commissioner that it is authorized to do so pursuant to the *ATIPPA, 2015*.

Statutes Cited: *Access to Information and Protection of Privacy Act, 2015*, ss. 2, 3, 61-72, 73-80, 97.

Authorities Relied On: BC OIPC *Order F07-10, Board of Education of School District No. 75*, 2007; ON IPC *Halton Catholic District School Board*, 2015; NL OIPC *Report 2007-008*; NWT IPC Review Recommendation 16-145, 2016; NS OIPC Investigation Report IR17-01 - Video Surveillance at the Cape Breton-Victoria Regional School Board, 2017; NL OIPC Report A-2018-005.

Other Resources: NL OIPC *Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador*, June 2015; NL OIPC *Guideline for Privacy Impact Assessments*, June, 2015; NL Department of Justice and Public Safety, ATIPP Office, *Protection of Privacy Policy and Procedures Manual*, June 2015, British Columbia Guidance Document, *Employee Privacy Rights*

File: 0055-094-17-001

I BACKGROUND

[1] In September 2017 our Office received a complaint under the *Access to Information and Protection of Privacy Act, 2015* ("the *ATIPPA, 2015*" or "the *Act*") expressing concerns about the collection and use of personal information recorded by the video surveillance system operated by the Town of Paradise ("the Town"). Our Office notified the Town of the complaint and asked a number of questions about the video surveillance system, the reasons for its installation, the handling of the information obtained, and the Town's policies, procedures and plans relating to the system. We attached a copy of our *Guidelines for Video Surveillance by Public Bodies* to our request for information.

[2] The Town responded in October 2017, providing most of the information we requested. Once we reviewed the response, we determined that more information was necessary. We sent the Town a second letter on December 6, 2017 seeking more detail in the areas of legislative authorization and operational necessity for the video surveillance system. We also asked about access controls and security, in order to determine whether adequate safeguards existed to protect against improper access, use or disclosure.

[3] We requested a significant amount of information in our December 2017 letter. The Town asked for and was granted additional time, until January 8, 2018, to respond. That response, however, never arrived. Instead, we received a letter on January 17, 2018 from the Town, objecting to our jurisdiction and procedures. Although we responded to the Town's objections, it did not provide additional information.

[4] The Town's failure to provide the requested information precluded any possibility of informally resolving the complaint. The Town's lack of cooperation does not relieve me of the duty to complete the investigation and to prepare this Report pursuant to section 77 of the *ATIPPA, 2015*.

II DECISION

[5] In many regions of our Province, it is increasingly unlikely that residents can leave their homes without a video surveillance system recording their movements. From our convenience stores to our workplaces, schools, hospitals, and everywhere in between, our images (and sometimes voices) are recorded. Some of those images are so grainy that people are not identifiable; however, improvements in technology increase the likelihood of identifying the people recorded. When people are identifiable, their right to privacy is impacted. When a public body, such as the Town of Paradise, operates the video recording system in question, it must comply with the *ATIPPA, 2015* regardless of any complaint or lack thereof. As stated in our *Guidelines for Video Surveillance by Public Bodies*, public bodies may only collect personal information as authorized by section 61 of the *ATIPPA, 2015*.

[6] "Recorded information about an identifiable individual" is personal information as defined in section 2(u) of the *ATIPPA, 2015*. The Town objected that if the individuals recorded were not identified, it would not be their personal information. While we agree that it requires additional information to link a person's image to a name, that linkage is often not difficult. That is why privacy statutes refer to "identifiable" rather than "identified" individuals in the definition of personal information. If the person in an image could potentially be identified the image is their personal information.

[7] Our Report 2007-008 referenced this issue:

> *A record contains information about an identifiable individual when there is a reasonable expectation that the information in the record by itself, or in combination with information from sources otherwise available, can lead to an identification of the individual involved.*

A person is also identifiable from a record where they are identifiable by those familiar with the particular circumstances or events contained in the record. This is a particularly relevant consideration when the individuals concerned are employees and members of the public who use Town facilities.

[8] The Town questioned our legislative authority to require that it provide information relevant to its compliance with section 61 of the *ATIPPA, 2015*. First, the *ATIPPA, 2015* sets out requirements for the collection, use, and disclosure of personal information by public bodies. Municipalities must comply with these requirements.

[9] Second, this Office functions as an independent statutory body that oversees compliance with the *ATIPPA, 2015* through several means, including the investigation of privacy complaints. Section 97 explicitly empowers the Commissioner to require, and obliges public bodies to produce, "…any record in the custody or under the control of a public body that the Commissioner considers relevant to an investigation". The Town asserted that procedural fairness entitled it to a complete copy of the complaint. Section 73(5) of the *ATIPPA, 2015* requires only that we provide a summary of the complaint, which the Town received. The complainant requested anonymity. Nothing about this investigation required identifying the complainant to enable the Town to respond. Ultimately, the investigation relates to how and why information is being collected by the Town through its video surveillance program, and other questions relevant to determining compliance with *ATIPPA, 2015*, regardless of who filed a complaint. The threshold for the commencement of our investigations is low. Section 73 allows individuals who believe on reasonable grounds that their "personal information has been collected, used or disclosed by a public body in contravention of this Act" to file a privacy complaint with the commissioner. As referenced in our Report A-2018-005, the Town recently confirmed that it did not even need to look at the recordings to determine that they captured identifiable individuals.

[10] The Town also objected to our process, taking the position that our investigation created a "reverse onus" on the Town to justify its collection of purported personal information without first receiving evidence of their failure to comply with the *Act*. Providing detailed allegations in advance of requiring a response is generally associated with proceedings that can result in imposition of a penalty such as a fine or imprisonment. Our investigative processes, in an administrative law context, have a foundation in the *Act* and are adapted to a context in which all public bodies must comply with the *Act* independently of any allegation of a breach. We can only make recommendations and public bodies can ask the Court to declare that they do not have to comply with those recommendations. The Town's insistence

that we import procedures consistent with those in court proceedings would subvert the purposes and functions of the *Act.*

[11] Our initial letter to the Town in September 2017 sought:

1. *The number and location of video surveillance cameras currently employed, in all facilities, by the Town of Paradise, including the Paradise Town Hall and associated buildings, the Paradise Double Ice Complex, the Rotary Youth and Community Centre;*

2. *The number of cameras currently employed in each facility, including:*
   a. *the number in public areas,*
   b. *the number in staff only areas,*
   c. *the number of exterior and interior cameras;*

3. *Copies and locations of any video surveillance signage;*

4. *The capabilities and features of each of the cameras (i.e. audio, video, movable, zoom, hidden, interior or exterior, wireless, permanent or moveable, motion detected or always on, etc.);*

5. *The reasons the cameras were originally installed (this may vary by camera);*

6. *Are the videos livestreamed, recorded, or both?*
   a. *Who has access?*
   b. *How are they able to access the cameras?*
   c. *Has footage ever been used, and if so, for what reason?*

7. *The length of time the cameras have been in place, and whether any re-evaluations have been conducted to assess whether they are still needed;*

8. *Are there plans to install video surveillance cameras in locations where there are none at present? If so, please provide the same information for such cameras as requested above;*

9. *If footage has ever been used by the Town or shared with third parties, please provide details, including how the Town processes third party requests;*

10. *If covert surveillance has ever been used, details of same;*

11. *Copies of any video surveillance policies, and any other Town policies that may relate to this complaint;*

12. *Any plans or procedures you may have developed to deal with potential breaches of personal privacy by the Town;*

13. *Any additional commentary or information that you feel will assist the Office.*

[12] The Town provided information responsive to that request, including:

- that it operates 87 video cameras, distributed among the Town Hall, the Town depot, recreation facilities and the community centre;
- most of the cameras were installed and activated in December 2016;
- there are 69 cameras in public areas, while 18 are in staff-only areas;
- there are 64 cameras located outside buildings, and 23 are inside; and
- there are 16 signs posted in various locations advising people that the area is under video surveillance.

[13] The Town advised that the cameras are permanently mounted, with zoom capability. There is both live feed and video recording, but no audio. Each camera is motion-activated – that is, they only record on detecting motion.

[14] The live stream from the video cameras is sent to the computers of 25 Town staff in administration, public works and recreation. Seven of those have access to all areas, while others have access limited, for example, to the depot, the arena or the community centre. Most of the individuals who have access to all cameras also have access to the recorded information. Access requires entry of a username and password on each individual's work computer. The system logs all accesses by each user.

[15] The Town provided our Office with a copy of its Video Surveillance Policy, adopted in September 2016 and revised in November 2017. The policy outlines:

- criteria for siting of cameras;
- where and how information is to be stored, and for how long;
- what equipment is to be used; and,
- who will have access to the information collected, and for what purposes.

[16] The Town's response and its Video Surveillance Policy state that the safety and security of workers, visitors, users and the public is of the utmost importance. It advised that it installed the surveillance system following bomb threats, false activation of fire alarms, theft, vandalism, property damage and complaints of illegal activity. The policy states that the purpose of video surveillance is to provide additional security to Town workers, users, visitors to Town facilities, and Town property, while complying with the *ATIPPA, 2015*. The Town did not explain how video surveillance of staff-only areas would accomplish this purpose or why it was necessary.

[17] The Town stated that it previously used recorded information on two occasions: once during the investigation of a potential theft, and once in the investigation of potential damage to a vehicle in the Town Hall parking lot. No other details, such as whether the Town collected useful information from the recordings, whether individuals involved were identified or whether personal information was disclosed to other persons, were provided to us.

[18] After reviewing the initial information provided by the Town, we determined that additional information was needed to assess whether the Town was authorized by the *ATIPPA, 2015* to collect personal information via its video surveillance systems. Accordingly, on December 6, 2017 we wrote a detailed follow-up letter to the Town. Unfortunately, no further information was forthcoming.

[19] The *ATIPPA, 2015* in Part III (Protection of Personal Information) limits the purposes for which personal information may be collected:

> *61. 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*.

[20] There is no apparent provincial statutory authority for the Town to collect personal information via video surveillance. The Town is not engaged in law enforcement as defined

in section 2(n) of the *Act*. As such, in order for the collection of personal information using a video surveillance system to be authorized by subsection (c), the collection of that information must relate directly to and be necessary for an operating program or activity of the Town.[1]

[21] The operating programs and activities of a municipality like the Town of Paradise are quite broad, consisting at a minimum of the provision of municipal services, including administrative and recreational services, to the residents. Appropriately, the Town's operations, programs and activities are conducted with regard for the safety and security of individuals and of Town property.

[22] The video system covers the Town Hall, the depot, the community centre and the recreational buildings. The question becomes, how does the collection of people's personal information through video surveillance relate to the provision of municipal services at those locations, and why is the collection of that information necessary? The Town must be able to answer those questions in order to demonstrate that its collection of personal information via its video surveillance system is authorized by the *Act*.

[23] The Town states that the video surveillance system was installed due to a number of concerns for safety and security. Concerns must be founded on data. The Town installed these systems in 2016 and broadly distributed the cameras. What occurred in or leading up to 2016 that led to the decision to employ these cameras as a component of the Town's operating programs?

[24] Even if there are reasons to employ video surveillance as part of the Town's programs, each collection of personal information (ie, each camera) must also be necessary within the meaning of section 61(c). As our *Guidelines* state, before a public body can decide to install and operate a video surveillance system, there must be "… a real, pressing and substantial

[1] For useful discussions of the application of these principles see NWT IPC Review Recommendation 16-145, 2016; NS OIPC Investigation Report IR17-01 - Video Surveillance at the Cape Breton-Victoria Regional School Board, 2017.

problem which is ongoing in nature that has not and cannot be mitigated by other less privacy intrusive measures." The *Guidelines* go on to say:

> *One incident, no matter how serious or severe, does not constitute a real, pressing and substantial problem. Nor does a series of minor incidents constitute a real, pressing and substantial problem. Public bodies must determine if there is a problem that requires the use of CCTV systems.*
>
> *Specific, ongoing and verifiable reports of incidents of crime, public safety concerns, or other compelling circumstances are required to proceed. This does not include anecdotal evidence or speculation. The purpose of the proposed CCTV system must be clear, and the use of CCTV must be necessary to address the specific incidents or problems which have been identified. This means that less privacy-invasive measures must be evaluated, and where practical, implemented, to see whether the issue can be addressed through such measures, prior to the installation or usage of a CCTV system. Less privacy-invasive measures should be utilized unless they are ineffective or not feasible.*

[25] This view is consistent with those expressed in other jurisdictions with similar legislation. The Information and Privacy Commissioner of BC discussed the meaning of "necessity" in the context of the collection of personal information in *Order F07-10, Board of Education of School District No. 75*:

> [48] *The collection of personal information by state actors covered by FIPPA––including local public bodies such as the Board––will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.*

[26] Similarly, Ontario's Commissioner in *Halton Catholic District School Board* adopted a decision of the Court of Appeal on that point:

> *In Cash Converters Canada Inc. v. Oshawa (City) the Ontario Court of Appeal adopted the following approach with respect to the application of the necessity condition and stated:*
>
> *In cases decided by the Commissioner's office, it has required that in order to meet the necessity condition, the institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within*

> *the meaning of the Act. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.*

[27] It is clear that in order to complete the above analysis, public bodies must compile a significant amount of information in order to assess whether it is necessary to collect personal information via video surveillance systems. This information must be compiled before activating video surveillance systems and must made be available if requested by this Office.

[28] Any public body contemplating the use of video surveillance systems should conduct a Privacy Impact Assessment ("PIA") as part of its decision-making process. For municipalities, privacy impact assessments are voluntary, but they are quite a useful tool for ensuring compliance with the *Act* when considering potentially privacy-invasive measures such as video surveillance.

[29] As a component of our investigation, we sought information regarding the Town's bases for concluding that video surveillance was necessary. We therefore asked the Town a number of additional questions, focused on the stated reasons for the installation of the system (bomb threats, false activation of fire alarms, theft, vandalism, property damage and complaints of illegal activity). The information we sought included:

- *how many documented incidents of each kind have there been in recent years?*
- *what were the dates?*
- *clarify the incidents with detailed information;*
- *assess the harm that resulted;*
- *explain what needed to be done to deal with the problem;*
- *explain what other measures were tried first, or at least considered;*
- *explain why those other measures did not work;*
- *explain how the use of video surveillance was expected to deal with the problem;*
- *show whether the use of video surveillance did in fact resolve the problem.*

[30] We also advised that this assessment applied to each of the locations at which video cameras were installed, because it is possible that for some kinds of problems, in some

locations, cameras will be a solution. In other cases cameras may not be authorized. Therefore, we asked that the Town describe in detail each of the locations in which cameras were installed, and explain the reasons for placing a camera in that location.

[31] While we sought a significant amount of information, it is information that the Town should have assembled prior to installing the cameras, in order to ensure that its video surveillance program was in compliance with section 61 of the *ATIPPA, 2015*. The Town failed to provide this information when requested as part of our investigation.

[32] The Town referenced theft from, or damage to vehicles in one of its parking lots as one of the reasons its cameras were installed. The first step in the assessment is to determine the extent of the problem. If there was only one incident, that would not qualify as a persistent problem that would render cameras as necessary within the meaning of the *Act*. On the other hand, a persistent history of vandalism or thefts from vehicles could be an example of a real, pressing and substantial problem at the locations where those incidents are occurring.

[33] Confirming the existence of a continuing theft or vandalism problem is in itself not enough. The next question is whether less intrusive means could address the concerns. For example, is parking lot lighting adequate? Does the Town have security personnel or other staff on duty at times when parking lots are in use? Can their rounds or other duties be adapted to increase monitoring of the parking lots? Were the police asked to conduct additional patrols in areas where vandalism is occurring? Even if other less intrusive measures had been attempted and proven inadequate, additional questions must be asked. What is the minimum number of cameras that might be required for this purpose? Are they needed 24 hours a day, or only during hours when the location is unoccupied? Are the cameras located only in areas where they can be justified?

[34] As previously noted, 18 of the cameras are installed in “staff-only” areas. On what bases did the Town conclude that these cameras were necessary and that other less intrusive means were insufficient? To any reasonable observer it raises the possibility that at least some of the cameras are located with a view to monitoring the activities of staff. The Town’s

employees have rights in regards to the privacy of their personal information. Video surveillance might be convenient to employers but it is a last resort measure, not a first. As noted in British Columbia's guidance document, *Employee Privacy Rights*: "Employers must carefully weigh the privacy harm when considering the use of video surveillance. A video camera cannot – and should not – replace adequate employee supervision." Moreover, section 66 of the *Act* provides that information collected for a specific purpose may not be used for another inconsistent purpose. For example, information collected for security purposes cannot be used to monitor employee productivity.

[35] The Town may have had some of these considerations in mind when it referred us to the fact that it is a unionized workplace, citing the "KVP Rules". These rules, familiar to labour arbitrators, set out the law applicable to employer rules and policies, including the requirement that policies must be reasonable. The Town argued that since the union had not grieved the Town's Video Surveillance Policy, it must be regarded as reasonable. Whether something is reasonable in a labour relations context is not determinative of compliance with any provision of the *ATIPPA, 2015*. Finally, section 75 vests discretion in the Commissioner to determine whether any other proceedings might be more appropriate than an investigation pursuant to the *Act*.

[36] The Town's failure to respond also limited information available to us to assess the unauthorized use and disclosure of the recordings from its video cameras. From the available information, it appears that the cameras are live streamed and recorded, and that access to the system is by username and password on the computers of all 25 "authorized personnel". Without further information, it appears that there could be as many as 25 monitors, in various locations in Town premises, continuously streaming the feed from any number of cameras at any given time. Access to personal information should be limited to employees who require it to perform duties of their employment. Allowing unnecessary access increases the likelihood of inappropriate use and disclosure.

[37] The Town's policy and its initial response indicate that the video surveillance system operates through the Town's computer system. The Town provided no details about whether the cameras, the other equipment and the monitors are hard-wired, whether they are linked

through wireless connections or whether the storage is on the Town's equipment or "in the cloud." It is also not clear whether any of the "authorized personnel" have remote access, or whether any of the pathways through which digital information travels are encrypted to prevent unauthorized access. This information is critical to assessing compliance with the *ATIPPA, 2015*.

III CONCLUSIONS

[38] The Town's failure to provide the requested information is a contravention of the Town's obligations under section 97 of the *ATIPPA, 2015*. On the available information, I conclude that the Town is not authorized to collect personal information via its video surveillance systems.

[39] One of the premises of the *ATIPPA, 2015* is that public bodies must satisfy all requirements with respect to the collection of personal information. This requirement is interpreted similarly in the ATIPP Office's *Protection of Privacy Policy and Procedures Manual* which states, at p. 20:

> *A public body must demonstrate that it is meeting the requirements set out in section 61 relating to its collection of personal information. Where the public body cannot demonstrate that it is meeting the requirements, it should revisit the policy of collecting certain personal information*.

[40] We recently issued Report A-2018-005 in which we recommended that within 90 days the Town acquire the storage capacity to preserve all video surveillance recordings in compliance with its Video Surveillance Policy, and that it acquire or source the capacity to de-identify persons recorded by its surveillance cameras. The Town subsequently agreed to do so. Those recommendations may appear contradictory to the below recommendation that the Town cease conducting video surveillance. Report A-2018-005 addressed access to the personal information in the recordings. Here we are dealing with privacy issues and the requirement for authorization to collect that personal information.

[41] If at some future point wants to recommence the operation of its video surveillance system (wholly or partly), this Report provides a roadmap to amassing the required information and the necessary analyses. Should the Town request our assistance or advice, we are more than willing to work with Town officials to ensure that any collection of personal information by the Town is authorized by the *Act*.

IV RECOMMENDATIONS

[42] Under the authority of section 76(1)(a) of the *ATIPPA, 2015*, I recommend that the Town of Paradise immediately cease collecting personal information via the Town's video surveillance system.

[43] As set out in section 78 of the *ATIPPA, 2015*, the head of the Town of Paradise must give written notice of his or her decision with respect to these recommendations to the Commissioner within 10 business days of receiving this Report.

[44] Dated at St. John's, in the Province of Newfoundland and Labrador, this 3rd day of April 2018.

Donovan Molloy, Q.C.
Information and Privacy Commissioner
Newfoundland and Labrador