OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report P-2021-002

May 4, 2021

Town of Happy Valley-Goose Bay

Summary: The Town of Happy Valley-Goose Bay initiated a body-worn camera ("BWC") program for municipal enforcement officers. As the Office of the Information and Privacy Commissioner had concerns with the program's compliance with the *Access to Information and Protection of Privacy Act, 2015* (*ATIPPA, 2015*), the Commissioner launched this own motion investigation after the program began collecting personal information. The Commissioner found that, while it appears that the Town has the authority to collect and use personal information for the purpose of law enforcement under sections 61 and 66 of *ATIPPA, 2015*, the scope of the municipal enforcement officer's duties are broader than what is contained within the definition of that term in section 2(n). Further, the Commissioner concluded that there were several outstanding concerns: the Town's statutory authority to disclose information; the Town's ability to use and disclose the minimum information necessary for the identified purpose; the safeguards in place; and the retention schedule. The Commissioner found that the Town's current program, although not currently active, is not in compliance with the requirements of *ATIPPA, 2015*. The Commissioner made a number of recommendations. Under the authority of section 76(1), it was recommended that the Town stop collecting, using or disclosing personal information using BWCs until such time that it can demonstrate full compliance with *ATIPPA, 2015*. Under the authority of section 76(2), it was recommended that the Town develop a privacy management program, complete a privacy assessment of the program, update the BWC policy to ensure compliance with *ATIPPA, 2015*, consult with the public regarding the proposed program, develop and execute a public communications plan regarding the program, and identify a redaction solution.

File #: 0055-124-20-002

Statutes Cited:

Access to Information and Protection of Privacy Act, 2015, SNL 2015, c. A-1.2, sections 2(n), 61, 62, 64, 65, 66, 68, 72.

Detention of Intoxicated Persons Act, RSNL 1990 c. D-21.

Highway Traffic Act, RSNL 1990 c.H-3, section 189.

Motorized Snow Vehicles and All-Terrain Vehicles Act and Regulations, RSNL 1990 c. M-20.

Municipalities Act, 1999, SNL 1999 c. M-24, sections 179, 419, 420, 421.

Town of Happy Valley-Goose Bay Violation Notice Regulations, Newfoundland and Labrador Regulation 13/15.

Urban and Rural Planning Act, 2000, SNL 2000 c.U-8, section 39.3.

Authorities Relied On:

NL OIPC Report A-2021-009; OIPC NL Report A-2021-014; BC OIPC Order F07-10; *R. v. Caines*, 2020 NLPC 13021207322; R. *v.* Oakes, [1986] 1 S.C.R. 103.

R. v. Laramee, 1972 CanLII 1365 (NWT TC)

Other Resources:

OIPC NL's Video Surveillance by Public Bodies in Newfoundland and Labrador; Office of the Privacy Commissioner of Canada's Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities; OIPC NL's PPIA/PIA Review Criteria; Town of Happy Valley-Goose Bay's Body-Worn Camera Policy PS0009; OIPC NL's Privacy Management Program Guidelines PrivacyManagementProgramGuidelines.pdf (oipc.nl.ca)

I BACKGROUND

[1] In March 2020, the Office of the Information and Privacy Commissioner (the "OIPC") learned through the media that the Town of Happy Valley-Goose Bay (the "Town") intended to use body-worn cameras ("BWC"). OIPC reached out to discuss this initiative with the Town on a number of occasions, not as part of an investigation, rather under the authorities available under section 95, which include:

- monitoring the practices and procedures employed by public bodies in carrying out their responsibilities and duties;
- commenting on the implications for access to information or for protection of privacy of proposed legislative schemes, programs or practices of public bodies; and
- taking actions necessary to identify, promote, and where possible cause to be made adjustments to practices and procedures that will improve the protection of personal information by public bodies.

[2] It soon became clear that efforts to use advocacy and persuasion had not had the desired impact. The BWC program had clearly been in operation, and we saw no indication that the Town's policies and procedures adequately addressed the collection, use and disclosure of personal information through that program, nor did we see evidence of a clear intention and specific time frame within which to effect such changes. Given the fact that these concerns remained and the initiative had actively collected personal information, OIPC notified the Town on December 1, 2020 that it was opening an own motion investigation under the authority of section 73(3) of the *Access to Information and Protection of Privacy Act, 2015* ("*ATIPPA, 2015*").

[3] Our intention in launching this investigation was to bring to bear the formal investigative authority under *ATIPPA, 2015*, so that the Town would no longer be in a position to ignore our questions or delay responses. Unfortunately, the Town was slow responding to requests for information on the program even once the investigation had been launched. The Town's initial submission was received promptly, however did not contain the level of detail necessary to assess compliance with the *Act*. Our Office followed up with a meeting and correspondence

in early January and, when no response was received, it became necessary to take the extraordinary step of writing the Town in correspondence dated January 26, 2021 to remind it of OIPC's authorities under section 97 (production of documents) and the Office's ability to issue a summons in accordance with section 9 of the *Public Inquiries Act* compelling the Town's cooperation.

[4] The Town informed OIPC that the BWC program is currently on hold and no personal information is currently being collected using BWCs, however OIPC remains unclear on what "on hold" means. While the Town's second submission, dated February 25, 2021 indicated that OIPC had been informed that the program had been on hold since October 2020, this contradicts the Town's first submission that stated that one BWC had not been used since October 2020 because of an ongoing investigation and the other was in use until November 20th. It is OIPC's understanding that, at least initially, the BWCs were not being used because of circumstances of the staff that use the BWCs, not because the Town formally suspended the program. It remains OIPC's understanding that the Town Council has not formally suspended the program.

[5] During the course of this file, and immediately prior to launching the investigation, there were changes in Town management and four senior management positions are currently vacant. While these vacancies would likely have impacted the Town's capacity to respond to our investigation, it also underscores the fact that public bodies must ensure that they have not only the organizational capacity to purchase new technology but also that they have the capacity to operate that technology within the applicable regulatory environment, including the need to document decisions and processes to ensure business continuity can be maintained during periods of staff turnover. The Town has indicated its intent to reinstate the program, noting "despite the Town being keen to get the BWC Program back up and operational as soon as possible, resources dedicated to this effort have been restricted."

[6] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 74(2) of *ATIPPA, 2015*.

II PUBLIC BODY'S POSITION

[7] The Town provided our Office with two submissions containing some details of the program and citing *ATIPPA, 2015* provisions upon which it is relying for its authority to collect, use and disclose personal information. We will examine each authority later in this Report. The Town also notes that the BWC program has been on hold since October 2020, and indicates, "[t]here will be important changes to the program that was put in place earlier in 2020, and the Town looks forward to the OIPC's input and recommendations."

[8] The Town asserts that the BWC program is necessary for the effective enforcement of municipal and other regulations. The Town's boundaries include remote, forested areas with low populations and many enforcement calls involve close contact with individuals. Recordings from BWCs can assist both enforcement and individuals involved in incidents and the Town notes, with regard to the duties of the Municipal Enforcement Officer (the "MEO"):

> *He also regularly attends to calls involving one officer and multiple individuals, a situation which doesn't allow for easy recording by the officer of investigation and interactions. This also provides the opportunity for multiple witnesses to contest his recollection of events, regardless of the truth. He also requires good records of alleged violations for prosecution purposes.*
>
> *Similarly, the existence of accurate, objective records can actually help the individuals whose information is recorded in them if they are wrongly accused of violations or misconduct. It can even help prevent unnecessary prosecutions from proceeding.*

[9] The Town's submission recognizes the importance of trust and accountability in law enforcement officials and states, "[u]nfounded allegations of misconduct and complaints about the behaviour of enforcement officers have fed an erosion of trust in the Town's law enforcement for many individuals." This issue has been compounded by comments made by individuals on social media. The Town also highlights the overall benefits of BWCs:

> *In addition to direct law enforcement purposes, it is acknowledged by police forces, government bodies, the public, and academics that BWC programs can help promote professionalism, good behaviour, and accountability in law enforcement officers. They also help to fairly investigate complaints of officer misconduct.*

III ISSUES

[10] The issues to be dealt with in this Report are:

1. Whether the Town has the authority to collect, use and disclose personal information using BWCs;
2. Whether reasonable safeguards are in place as required in section 64;
3. Whether the Town's notification meets the requirements of section 62(2);
4. Whether a retention schedule has been established as per section 65;
5. Whether steps have been taken to ensure that the minimum amount of information necessary is used or disclosed, as per sections 66(2) and 68(2);
6. Whether appropriate processes are in place to ensure the Town is able to manage privacy complaints and access requests for the information captured by BWCs;
7. Whether appropriate processes are in place to review and approve Town initiatives with privacy implications.

[11] In addition to *ATIPPA, 2015*, OIPC analysis in this section will consider the Office of the Privacy Commissioner of Canada's Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities, which was developed in collaboration and consultation with provincial privacy and access offices across the country, including Newfoundland and Labrador. While recognizing that there are legitimate situations for the use of BWCs, the guidance calls on law enforcement agencies to evaluate, in each specific context and for the specific intended purposes and uses, whether the expected benefits outweigh the impact on privacy. Important steps include public awareness of the initiative, appropriate safeguards (including encryption, restricted access to recordings and strict retention periods), program specific policies and procedures, and any secondary uses (such as officer training). The guidance concludes:

> *BWCs record not only the actions and speech of an individual, but also individuals' associations with others within recording range, including friends, family members, bystanders, victims and suspects. The recording of individuals through the use of BWCs raises a significant risk to individual privacy, and LEAs [Law Enforcement Agencies] must be committed to only deploying BWCs to the degree and in a manner that respects and protects the general public's and employees' right to personal privacy.*

1. Authority to Collect, Use and Disclose

Authority for Collection

[12] The Town has identified sections 61(b) and (c) as the sources of its authority for the collection of personal information through the BWC program, although the Town stated in part that "[t]he primary reasons [sic] for the BWC program and the recording of interactions between the Town's enforcement officers and members of the public are law enforcement purposes." This Report examines both sections in turn below.

Collection of Information for Law Enforcement

[13] Section 61(b) authorizes the collection of information for the purpose of law enforcement, which is defined in section 2(n):

> *2(n) "law enforcement" means*
>
> *(i) policing, including criminal intelligence operations, or*
>
> *(ii) investigations, inspections or proceedings conducted under the authority of or for the purpose of enforcing an enactment which lead to or could lead to a penalty or sanction being imposed under the enactment;*

[14] The Town purchased three BWCs for use by municipal enforcement staff; one was used by the MEO, one by the Animal Control Officer (the "ACO"), and the third was securely stored. Council has the authority to appoint one or more MEOs under section 179(1) of the *Municipalities Act, 1999*, which states:

> *A municipal enforcement officer appointed under subsection (1) has the powers of a member of the Royal Newfoundland Constabulary with respect to the enforcement of this Act and regulations made under this Act within the municipality for which he or she is appointed.*

[15] As the Town's first submission did not cite the authority for the collection, OIPC conducted its own assessment of 61(b) and communicated this to the Town. OIPC concluded that the Town does have some responsibilities that appear to fall into the definition of law

enforcement, the majority of which are outlined in section 3 of the *Town of Happy Valley-Goose Bay Violation Notice Regulations under the Municipalities Act, 1999:*

> *3. The town council of the Town of Happy Valley-Goose Bay may issue violation notices with respect to a failure to comply with a provision of the following regulations enacted by the town council under the Municipalities Act, 1999 or the Urban and Rural Planning Act, 2000 :*
>
> *(a) Anti-Litter Regulations ;*
>
> *(b) Dog/Cat Regulations ;*
>
> *(c) Happy Valley-Goose Bay Development Regulations ;*
>
> *(d) Noise Regulations ; and*
>
> *(e) Water and Sewer Regulations .*

OIPC's analysis also examined sections 419 and 420 of the *Municipalities Act, 1999*, which establish penalties or sanctions for certain activities.

[16] The Town's second submission provided additional details of law enforcement activities:

> *The Town maintains the power to issue fines for and prosecute violations of its regulations pursuant to sections 420 and 421 of the Municipalities Act, 1999. The Town's Municipal Enforcement Officer and Animal Control Officer are charged with investigating, issuing fines for, and prosecuting violations of Town regulations, as well as those under various other acts and regulations. See, for example, The Highway Traffic Act, and the Motorized Snow Vehicles and All-Terrain Vehicles Act and Regulations.*

[17] The Town notes that its Traffic Regulations have been enacted under section 189 of the *Highway Traffic Act* and further states:

> *... Under the same section, the Town has appointed the Municipal Enforcement Officer as peace officer to enforce those regulations, which necessitates collection of personal information, as would any criminal, quasi-criminal, or regulatory investigation.*

[18] Section 189 of the *Highway Traffic Act* establishes the authority of the Minister of Transportation and Infrastructure to make orders that delegate a municipal council the power to make regulations, and for municipal council to appoint a peace officer to enforce the regulations. That being said, this only applies to the regulations created under section 189(1)

of the *Highway Traffic Act* that the Minister has delegated to a municipal council. While the Town verbally indicated that it had documentation that authorized activities like traffic stops, OIPC requested a copy and none has been provided to date. In absence of supporting documentation, OIPC cannot validate that the Town has the authority to enforce provisions under the *Highway Traffic Act*.

[19] If the Town does have authority to enforce provisions of the Act, the Town's MEO would be considered a Peace Officer, but only for the limited purpose and circumstance described above; that is, to carry out a prosecution of an offence under the *Highway Traffic Act*, such as issuing tickets for traffic violations within Town boundaries.

[20] It is important to discuss the term "Peace Officer" further, as there could be confusion. The Town's website states, "Community Constables are Peace Officers as defined under the Criminal Code, employed for the preservation and protection of the public peace as well as Civil Service." OIPC is not confident that this statement is accurate, based in part on *R. v. Laramee.* This case examined the definition of "peace officer" in the Criminal Code in conjunction with the *Interpretation Act*. The case concluded, in part

> *I therefore hold that Sergeant Cook was not a "peace officer" for the purposes of s. 235 of the Criminal Code, and that he is to be regarded as such under s. 2 of the Criminal Code, and related provisions, only in so far as may be necessary for the due performance of his duties of by-law enforcement.*

While MEOs may be designated as Peace Officers under some legislation for specific activities, the term does not apply in all circumstances.

[21] The Town brought up a number of other examples that, while understandably considered by the Town to be enforcement matters, do not appear to meet the definition of law enforcement in *ATIPPA, 2015*. For example, when discussing the *Detention of Intoxicated Persons Act*, the Town states, in part, "[the *Act*] does not itself provide for penalties, but regularly allows the Town's Municipal Enforcement Officer to assist the RCMP in Criminal Code investigation and enforcement within the Town's boundaries." The Town appears to believe that section 179 of the *Municipalities Act, 1999* makes their MEO a "municipal police officer" and thus a "peace officer" under statutes such as the *Detention of Intoxicated Persons Act*.

However, the *Municipalities Act, 1999* only confers the authorities of a police officer on an MEO with respect to enforcement of the *Municipalities Act, 1999* and its regulations, not in general. So it remains unclear whether a range of the MEOs activities can indeed be characterized as law enforcement as defined in *ATIPPA, 2015*. The Town has not adequately demonstrated by reference to and interpretation of the applicable statutory provisions that this meets the definition of law enforcement as established in *ATIPPA, 2015* or even how it has determined that MEOs fall under the definition of "peace officer" under this Act. The Town further stated, "[t]his, along with the Noise Regulations, may inform your assessment of the Municipal Enforcement Officer's description of responding to calls about groups of people drinking outdoors within the Town." Again, this is not sufficiently specific to explain how these activities may fall under the definition of law enforcement in the *ATIPPA, 2015*.

[22] The ACO is responsible for issuing violation notices in areas directly related to the Animal Control position, including dog/cat regulations and noise regulations (*Town of Happy Valley-Goose Bay Violation Notice Regulations*). The ACO's job description gets very specific under duties and responsibilities:

> *Under the authority of section 421.3 of the Municipalities Act, 1999 and section 39.3 of the Urban and Rural Planning Act, 2000, responsible for issuing violation notices in areas directly related to the Animal Control position including: 3 (b) Dog/Cat Regulations and (d) Noise Regulations.*

[23] In the course of our investigation we examined the job descriptions of both the MEO and ACO. Both contained some roles and responsibilities that may meet the definition of law enforcement in *ATIPPA, 2015*, but they also contained many that do not. This is acknowledged in the Town's second submission, which notes that this is common with most law enforcement and police officers, stating:

> *Crime prevention and positive public interactions are what the Town would prefer its officers spend their days doing, however violations occur frequently, and these officers are the ones responsible for investigating them and taking appropriate actions to address them.*
> *...*
> *The fact that an officer has duties outside the scope of law enforcement does not preclude them from using a BWC for enforcement purposes.*

[24] The scope of duties of municipal enforcement officers is not a matter of concern. The issue to be determined, however, is what portion of those duties or activities falls within the scope of law enforcement and what falls outside of that scope. Those activities that clearly meet the definition of law enforcement, with specific reference to the statutory or regulatory authority underpinning them, would allow for the collection of personal information under section 61(b). Any duties or activities that fall outside of that scope would not allow for collection of personal information under 61(b). To date, the Town has not demonstrated an appreciation of this distinction or proposed how it will manage it in practice.

Collection of Information under an Operating Program or Activity

[25] The Town also cites section 61(c) as authority for the collection of personal information. Section 61(c) authorizes the collection of personal information when it relates directly to and is necessary for an operating program or activity of the public body. To show that the collection of personal information with a BWC is authorized by section 61(c), the Town must:

> (a) relate the collection of personal information using BWC to an operating program or activity of the Town, and
> (b) show that the collection of personal information is necessary.

[26] The Town's second submission states:

> *The collection of information in BWC footage relates directly to its law enforcement program and activities and it is necessary to ensure the good conduct of its officers and to gain or maintain public confidence in its officers, which requires ensuring that allegations of misconduct are fairly investigated and addressed. Additionally, being able to investigate allegations of misconduct and provide a safe workplace free from harassment, which the Town is obligated to do under occupational health and safety legislation, is essential to the well-being and safety of Town enforcement officers. On top of this, while the information collected about the officer's activities may be seen as quite sensitive, it would be collected with their consent, if not at their express request.*

[27] This statement broadly references several programs and activities but does not provide much description of these activities, nor does this statement fully encompass the scope of activities of enforcement officers when collecting personal information through BWCs. What we are missing is an adequate and specific description of these programs or activities and

how the collection of personal information relates to each, in order to then facilitate an assessment of the necessity criterion.

[28] The Information and Privacy Commissioner of British Columbia discussed the meaning of "necessity" in the context of the collection of personal information in Order F07-10:

> *[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.*

[29] Continuing with the above example of investigations of allegations of misconduct, this suggests that such investigations could not proceed in the absence of recordings from BWC. While BWC recordings could be utilized in conducting such investigations, should all of an enforcement officer's interactions be recorded for the few that may lead to such investigations? The Town's argument also mentions the provision of a safe workplace free from harassment, something required of all workplaces subject to occupational health and safety legislation. While a BWC could potentially record an incident of harassment, the Town has not presented any evidence that it would prevent such an incident from occurring. Furthermore, other municipalities and public bodies carry out harassment investigations as required, without the use of BWCs. What is special about the Town compared to other jurisdictions, or about the Town today compared to that of the past? It cannot just be that BWCs are now affordable and available. The answers provided by the Town seems to suggest that the MEO and ACO conduct enforcement alone in remote areas, there are trust issues with municipal enforcement, and there have been allegations of misconduct by municipal enforcement. The Town seems to be arguing that these problems are unique and/or new to the Town and justify the use of BWCs.

[30] The Town's submission does not provide sufficient details for OIPC to conclude that the collection of personal information using BWCs relates directly to, and is necessary for, an operating program or activity of the public body.

[31] In summary, although the Town has cited two authorities for its collection of personal information for the BWC program, OIPC cannot conclude, based on the information provided, that these authorities apply to all the personal information being captured by the BWCs. Further, the Town has not identified the specific activities that fall under each authority. This is essential, as the requirements when collecting personal information under the authority of law enforcement (section 61(b)) differ from those of section 61(c); this also applies to subsequent uses and disclosures of the information collected under those authorities. For example, there are different notification requirements when collecting under the law enforcement authority. While the program may be on hold at present, it actively collected personal information between July 2020 and November 2020. Based on the information provided by the Town during this investigation, OIPC has concerns that at least some of the recordings which were collected were not collected under the authority of *ATIPPA, 2015*.

Policy

[32] The Town's submission recognized that its BWC policy should be examined to ensure full compliance with legislative obligations and best practices, noting:

> *The Town continues to work on an updated BWC policy, consulting resources from privacy commissioners, legal and other commentary, as well as the programs of other police forces, including other Canadian police forces.*

While it may be helpful for the Town to consider resources or policies developed by Canadian police forces, they should exercise caution in doing so. Although municipal police forces may be common in some Canadian jurisdictions, they do not exist in this Province. Municipal Enforcement Officers are not part of a police force such as the RNC or RCMP. Their authority is limited to the specific statutory and regulatory powers prescribed, and the Town should therefore exercise caution in adopting policies or procedures developed by or for police forces.

[33] The Town's first submission included a number of policies: the Council approved policy that is currently in effect, and several draft policies. Although OIPC has been informed that the Town is working to update this policy, OIPC is examining the policy as it exists today.

[34] While the Town provided multiple drafts of proposed replacements, they contained significant deficiencies; for example, one contains references to Ontario legislation that is not

applicable here and misquotes *ATIPPA, 2015*. The Town may indeed have every intent of changing the policy to ensure legislative compliance, however this Office must review the current policy.

[35] The initial Body-Worn Camera Policy PS0009 was approved by Council in June 2020 and the MEO started using a BWC in July. In September 2020, the policy was amended to allow the ACO to use a BWC as well. Although the Town has informed OIPC that the BWC program is on hold, the policy itself remains in force. The policy states, in part:

> *The Policy has been developed to be in compliance with the Access to Information and Protection of Privacy Act (ATIPPA), 2015 and the Office of the Information and Privacy Commissioner (OIPC) guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador, 2015.*

[36] The policy is intended to govern the collection, use, disclosure, custody, control, retention, dissemination and disposal of personal information obtained using the BWC. Our review of the Body-Worn Camera Policy PS0009 raises some concerns and highlights gaps.

[37] For example, in the procedures section, a MEO activates recording functions and documents the existence of the BWC. There are separate but similar guidelines on when the BWCs should be activated by the MEO and the ACO, with both requiring that recording functions be activated "as soon as practically possible" in a number of general circumstances, including interactions that could result in a complaint, responses to calls for service and when advised to do so by the Town Manager. However, they are not required to tell the individual involved that it has been activated.

[38] Access to the recorded data is restricted, however the Town Manager and MEO have access to playback, copying and disclosing data. The Mayor and Councillors (a total of seven individuals) and the ACO will also have access to playback (though the latter only for recordings that pertain to ACO-related incidents). This seems to be an excessive number of individuals with access, and OIPC is unclear why elected officials would be provided with this access. In addition, without further information on the authority for these uses and disclosures, OIPC is unable to conclude that they are in compliance with the *Act*.

[39] The Town's second submission states, in part:

> *We can advise that, as of now, we do not anticipate that members of Council will have access to playback, and we anticipate that the people with access will be limited to the minimum number of staff necessary. Considered for playback are the Town Manager and/or Human Resources Manager and/or ATIPP Coordinator and/or the Municipal Enforcement Officer and/or Animal Control Officer. The number of staff with access to copying, disclosing, or redaction of videos will be very limited, if more than one. The Town is examining this decision closely, in consultation with the BWC policies of other forces, and commentary on best practices.*

[40] While the policy does establish some safeguards, during the course of this investigation there were instances of non-compliance identified. For example, the Town Manager is responsible for conducting a weekly review of five random recordings to ensure the BWC is being operated in accordance with policy, among other responsibilities. During our investigation, we requested the results of these random audits from when the program was operational from July 2020 to November 2020. It is our understanding that the five weekly random viewings did not commence until after the MEO was placed on administrative leave. The Town notes that the program was live for a short period of time before the MEO was placed on administrative leave, but it is concerning that no auditing occurred between July and October 2020 as required by the Town's policy.

[41] The policy also requires that a log is maintained to document accesses to and uses of recordings from BWCs. The audit log provided to OIPC showed two viewings of recordings by the MEO and one by the RCMP; there has been no deletion of recordings. The Town confirmed that there were no other viewings of the BWC recordings. The Town clarified the viewing by the RCMP was in relation to an investigation into a false complaint and a copy of the recording was not provided to the RCMP. One of the accesses by the MEO involved others, specifically an independent investigator and the Town Manager. While it could be argued that the Town Manager and MEO were using the recordings, any involvement of third parties would involve a disclosure, even if a physical copy was not provided. These discrepancies raise further concerns that the access log provided to this Office is incomplete.

[42] When asked to provide details of any policy compliance checks, the Town noted, "Since the program was put on hold in October 2020, there has been no program activity, so there is no more information on compliance to provide, other than that equipment and recordings have been stored as required."

Use of Personal Information

[43] As explained above, the Town has not demonstrated that it has the authority to collect personal information using BWCs to the extent intended by the Town. Therefore, discussions of legislative authority for use and disclosure will be much briefer. The Town indicated that it relies on sections 66(1)(a) and (b) as authorities for use. These provisions of the *Act* state:

> *66. (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 69 ;*
>
> *(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…*

[44] The Town's second submission states, in part:

> *…the Town suggests that use of the information collected, particularly about an officer, would be justified under section 66(1)(a) or 66(1)(b). The Town believes that the assurance of good conduct of officers, thorough and fair investigation of officer misconduct complaints, assurance of public confidence in Town enforcement officers, and provision of a safe and harassment-free workplace are consistent purposes. Also, in an investigation of a misconduct complaint, it is very possible the officer in question would consent to the use of their information.*

[45] With regard to section 66(1)(a), our assessment above concluded that the Town may have authority to collect information under section 61(b) for some activities. When the Town is in a position to clearly and accurately indicate which activities fall under law enforcement as defined by *ATIPPA, 2015*, it is possible that information collected under that authority could also be used under the authority of section 66(1)(a).

[46] In general, without a more robust discussion of how personal information relates to and is necessary for an operating program or activity of the Town, we cannot contemplate the use or

disclosure of any information collected under the authority of section 61(c). The Town has not demonstrated to our satisfaction that it has the authority to collect the information and therefore cannot rely on this as authority for use.

[47] As for section 66(1)(b), the above indicates that the Town has contemplated consent from the MEO and ACO. If it is intended that use of BWCs become a job requirement for persons occupying the MEO and ACO position, then consent is not a relevant consideration. Consent can only be voluntarily given – it cannot be mandated. Further, to rely on consent, the Town would require consent from every identifiable individual featured, either through voice or image, in the recordings. For example, there could be minors playing on the lawn in the background or people walking by the scene having a private conversation that, unbeknownst to them, is being captured. The contemplation of consent as part of this process further highlights the extent to which this program and how it would operate are only partially thought through.

Disclosure of Personal Information

[48] Disclosures and authorization for such disclosures were not discussed in detail in the Town's submission. OIPC had specific questions related to the authorities for disclosures listed in the initial submission, which included to the RCMP and the Court. The second submission states:

> *On the prospect of disclosure of BWC footage to third party law enforcement, the Town is considering how to address this as part of its review of the BWC Policy and invites commentary from the OIPC on this.*

[49] The Town should know its authority to disclose in various situations and have a specific policy to indicate the circumstances under which disclosure will be considered.

2. Reasonable Safeguards

[50] Safeguards generally involve administrative, technical and physical safeguards. The following examines the safeguards in place for the BWC program.

[51] Section 64 of *ATIPPA, 2015* states, in part:

> *64. (1) The head of a public body shall take steps that are reasonable in the circumstances to ensure that*
>
> *(a) personal information in its custody or control is protected against theft, loss and unauthorized collection, access, use or disclosure;*
>
> *(b) records containing personal information in its custody or control are protected against unauthorized copying or modification; and*
>
> *(c) records containing personal information in its custody or control are retained, transferred and disposed of in a secure manner.*

[52] The main administrative safeguard currently in place is the above-mentioned policy. It should be noted that, even if the Town improves the policy and addresses concerns raised by OIPC, it is important for the Town to ensure that individuals receive training on the policy and that the Town ensures compliance with the policy. Training should also educate end users on when it is appropriate to collect personal information using a BWC and staff on appropriate access to any footage. It must be noted that no amount or quality of training will be sufficient if the policy itself is incomplete.

[53] In addition to training on the policy, the Town must ensure that end users are trained on the BWCs themselves and their overall duties. While the MEO's job description requires them to have successfully completed, "the approved training program for Community Constable as offered by the RCMP, or an equivalent (or higher) approved police training program," qualifications for the ACO do not require the same background. No matter the professional background and experience of the MEO and ACO, training specific to the use of BWCs as utilized by the Town is required. The current policy requires that the MEO and ACO operate the BWC in accordance with the policy, which would generally involve training on the policy itself. Any training specific to BWCs should be more robust, for example, including a review of *ATIPPA, 2015* in the context of the program. To ensure material is understood, scenarios and examples should be used.

[54] While section 72 of *ATIPPA, 2015* does not require municipalities to complete a privacy assessment, they are still subject to compliance with Part III of the *Act*, which governs the

protection of personal information. Section 64(1) of the *Act* requires that public bodies take steps that are reasonable in the circumstances to protect personal information. When a new program is being introduced which has the potential for significant privacy impacts, conducting a PIA could be considered a step that is reasonable in the circumstances. Furthermore, privacy assessments are useful in ensuring and documenting compliance.

[55] With regard to technical and physical safeguards, the information collected does not transmit directly to the storage device. The data from the BWCs must be downloaded and the Town has an encrypted storage device for this purpose. Once downloaded, the data is deleted from the BWC and the BWC is returned to the officer. According to the information provided, physical access to the recordings is only available to the MEO and the Town Manager. The secure storage device is stored in a locked receptacle when not in use.

[56] While information is not encrypted upon collection, it is encrypted once it is transferred to storage, which should occur at the end of every shift. Only the MEO has the encryption passcode to enter the storage device.

[57] OIPC also inquired about any metadata created by or associated with the BWC recordings that is connected to an identifiable individual, such as transactional information about the user, the device, date, time, location, duration of the recorded activities, etc. No additional information was provided. OIPC was not informed about how the BWC is physically protected when in the custody of the MEO and ACO, or any features of the BWC that may or may not be used; for example, the manual indicates that the BWC can also be mounted and used as a dash cam.

[58] The Town's second submission did identify a number of safeguards that are being considered:

> *Among the measures being considered are:*
>
> - *Training requirements for the policy itself, all procedures under it, and technologies used as part of the program;*
> - *Mandatory warning, where practicable, for individuals being recorded;*
> - *Documenting of reasons for any permitted discretionary deviation from policy;*

- *Disciplinary action for non-compliance;*
- *Continued use of written and audio reports and other documentation procedures already in place;*
- *Redaction of visual and audio information of third parties;*
- *No use of biometric technology in handling or searching records;*
- *Elimination of recordings not used in ongoing investigations after 90 days;*
- *Limiting playback, copying, disclosure, redaction to very few individuals, as noted above;*
- *'Evergreen' clause requiring the re-evaluation of the policy at timed intervals and for compliance with legislative changes.*

[59] While it is positive that all of these things are being considered, they should be considered; decisions made about them; finalized into policy; and implemented, following training of key officials. Further, the above measures are a step in the right direction, however complete details of administrative, technical and physical safeguards will be required to determine if the program is in compliance with section 64.

3. Notification Requirements

[60] *ATIPPA, 2015* places requirements on public bodies when collecting personal information. Section 62(2) states:

> *(2) A public body shall tell an individual from whom it collects personal information*
>
> *(a) the purpose for collecting it;*
>
> *(b) the legal authority for collecting it; and*
>
> *(c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*
>
> *(3) Subsection (2) does not apply where*
>
> *(a) the information is about law enforcement or anything referred to in subsection 31 (1) or (2); or*
>
> *(b) in the opinion of the head of the public body, complying with it would*
>
> *(i) result in the collection of inaccurate information, or*
>
> *(ii) defeat the purpose or prejudice the use for which the information is collected.*

[61] The Town's Body-Worn Camera Policy PS0009 that is currently in force does not require that users inform individuals that the BWC has been turned on. In the procedures section, it states, in part, that recording functions must be activated "as soon as practically possible" and lists circumstances for same. It does not contemplate that different expectations may apply, depending if the information is being collected under the authority of 61(b) or 61(c).

[62] Policy aside, in a series of questions asked by OIPC and responded to by the MEO, the MEO noted:

> *Capturing the personal information of bystanders can happen in certain circumstances and unless in a confined space where there are only two individuals, the officer, and the individual being spoken to, it is almost impossible not to indirectly capture information of others in the vicinity. Training and awareness on the officer's part to be cognizant of this is important, along with public education that the officers are wearing the units, and notification to individuals being recorded have been happening since the activation of the units.*

[63] The MEO also noted that, when training the ACO, he discussed the indirect collection of personal information, and advised to, "always inform the individual that the interaction is being recorded preferably at the beginning of the interaction." This is a good practice that should be reflected in policy. No details of what training the Town offered to the MEO on the BWC program were provided.

[64] This, however, focuses on informing the individuals directly involved in an incident. Many entities that use BWCs undertake public education campaigns to better ensure citizens are aware of the presence of the BWCs and the potential that they are recording. Although it is indicated that public education regarding the BWCs was undertaken, no details of any efforts were provided by the Town. The Town's second submission states:

> *The Town echoes the OIPC's concerns about informing individuals of their being recorded, as well as the general awareness of the community about the BWC program. We can advise on the former concern that the enforcement officers will be obligated by the updated BWC Policy to advise any individual who is being recorded of that fact wherever practically possible. On the latter concern, the Town is closely considering further options for public awareness as part of its program review. Note that the BWC program has been getting widespread attention in the Town as an unintended but positive consequence*

> *of this investigation, an access complaint and investigation, and the events and investigation of an October 16, 2020 interaction involving the Municipal Enforcement Officer.*

[65] The public reacting to an operating program of the Town hardly represents a coherent public education campaign. OIPC asked about feedback from residents regarding the program. The Town's Manager of Public Relations noted that there were only posts and commentary on social media, such as Facebook. The Town had not received any correspondence by mail, email, direct message or telephone from the public regarding the use of BWCs. "The Town has through its Complaints Policy and Process for Delegations wishing to present to Council offered ample opportunity for the public to provide feedback."

[66] OIPC suggests that the lack of public feedback on the program should not be taken as indication that the public supports the program. Given that the majority of the public discourse on the initiative has stemmed from this investigation and the recording of the incident posted on Facebook, the lack of comment may just reflect the lack of public awareness. While we appreciate that the policy has been posted on the Town's website and there has been media coverage, the Town should take proactive steps to inform residents about its BWC initiative. It may also want to examine steps taken in other jurisdictions. For example, when the Montreal Police Service (SPVM) initiated a BWC pilot project, officers wore a special badge on their uniforms featuring an image of a camera to supplement verbal notification. Moreover, one of the issues the BWC initiative is designed to address is related to populations of people congregating in remote wooded locations. These groups may be facing housing issues and many may be dealing with addictions issues, and can generally be understood to be a vulnerable population unlikely to have access to these types of passive engagement in the same manner as non-vulnerable residents of the community. Moreover, according to media reports, many of these people are Indigenous and there is no indication of outreach to representatives of Indigenous organizations or governments. The Town needs to do better to engage the vulnerable populations whose personal information would be collected by this program.

4. Retention

[67] The Town's current policy establishes the retention schedule for the BWC recordings. It states that any recordings that have not been viewed for a period of 90 days should be deleted. Recordings that have been used, or are being used, in relation to an ongoing investigation or legal proceeding by the Town or law enforcement officials must be retained until the proceedings are concluded or a period not exceeding seven years.

[68] Section 65 of *ATIPPA, 2015* states:

> *65(1) Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.*
>
> *(2)A public body that has custody or control of personal information that is the subject of a request for access to a record or correction of personal information under Part II shall retain that information for as long as necessary to allow the individual to exhaust any recourse under this Act that he or she may have with respect to the request.*

[69] OIPC is not confident, based on the retention schedule established in the current policy, that compliance with the retention requirements of the *Act* have been appropriately considered. *ATIPPA, 2015* requires records that are subject to an access request to be retained for as long as necessary to allow for the individual to exhaust any recourse under the Act. In addition, public bodies must retain information used to make a decision that directly affects the individual for at least one year after using it. These do not appear to be considered in the existing policy.

5. Use and Disclosure of Minimum Personal Information

[70] Section 66(2) requires the Town to use the minimum amount of information necessary for the identified purpose. Minimizing use could include ensuring the minimum number of individuals use the information, that only the portion of the record needed is viewed and, in specific circumstances, redactions may be appropriate. Similarly, section 68(2) requires that the Town disclose the minimum amount of information necessary for the identified purpose; redaction software is critical in ensuring that the minimum information necessary is disclosed. While the Town doesn't currently possess audio or video redaction software, its second

submission notes that they are looking at options and states that they, “hope to purchase the software soon, but certainly before the BWC Program is restarted and BWCs are turned back on.”

[71] The Office of the Privacy Commissioner of Canada, in a 2015 guide, said the technology "poses serious implications for individuals' right to privacy," citing the ability of BWCs to pick up the conversations or likenesses of bystanders. In the absence of a plan to address redaction capabilities, it will be difficult for the Town to ensure that the minimum amount of personal information is used or disclosed.

[72] The purchase of redaction software is a positive and necessary step. The initial submission from the Town notes:

> *…complaints to Council regarding the handling of situations by the Enforcement Department have been largely fabricated or exaggerated to the point where the officer’s abilities and authority have been questioned. Footage of incidents able to be reviewed, after software redaction has been applied, would support, or refute these allegations thereby allowing Council to address the complaint.*

[73] This statement suggests that recordings will be used in complaint situations, if redactions are applied. According to the access log discussed above, uses and disclosures have already occurred without redactions.

6. Process for Privacy Complaints and Access Requests

[74] The Town’s submission did not provide much detail regarding access requests or privacy complaints under *ATIPPA, 2015*, other than indicating that the ATIPP Coordinator is the contact for both privacy complaints and access requests. The current policy refers all access to information requests involving BWCs to the ATIPP Coordinator, while requests for disclosure from law enforcement would be directed to the Town Manager. The ATIPP process, in particular when responsive records include video recordings, can be complex and the Town should have a clear policy detailing the process to be followed.

[75] Two recent reports from this Office address access requests involving video recordings and provide considerations and establish expectations for any public body using such

systems. Report A-2021-009 examined a request for access to recordings from the BWC and a vehicle camera. It is interesting to note that, while in the end we concluded that the record was excepted from disclosure, had the applicant been one of the individuals featured in the recording, then it would not have been except and the Town would be required to release the portion of the record containing the individual's personal information. In Report A-2021-014, which examined a request for video surveillance footage, we recommended that the public body acquire or source the capacity to de-identify persons recorded by its video surveillance systems.

[76] The Town did not provide any policy for the handling of access requests or privacy complaints. Further, the current BWC policy does not appear to contemplate privacy complaints, although it does state that the Town Manager will be responsible for investigating alleged privacy breaches.

7. The Appropriate Processes are in Place to Review and Approve Initiatives with Privacy Implications.

[77] Throughout our interactions with the Town, it became apparent that the Town needs to develop a Privacy Management Program, as recommended in Guidelines issued by my Office.

[78] Prior to commencing this investigation, we identified privacy assessments as important tools when undertaking such initiatives and even took the time to develop a series of questions to consider that were specific to BWCs. We explained that, while some public bodies are required to complete a PIA by section 72 of *ATIPPA, 2015*, the Town of Happy Valley-Goose Bay is not. However, the Town is expected to be in compliance with Part III – Protection of Personal Information - and a PIA can assist with this endeavor. The Town did not indicate that it had conducted a PIA on its BWC initiative.

[79] OIPC's PIA guidance also recommends that any public body considering a program that has privacy impacts complete the four-part test articulated by the Supreme Court of Canada in *R. v. Oakes*. This test is a solid starting point when considering the adoption of a new technological solution that involves the collection, use and disclosure of personal information. The Oakes test is a useful framework to apply because privacy rights have been recognized

under the Charter, so at a more foundational level, even beyond *ATIPPA, 2015*, there are some fundamental questions:

- Is the measure demonstrably necessary to meet a specific need?
- Is it likely to be effective in meeting that need?
- Is the loss of privacy proportional to the need?
- Is there a less privacy-invasive way of achieving the same end?

[80] As part of this investigation, OIPC inquired about the Oakes test. Each question is discussed below.

Is the Measure Demonstrably Necessary to Meet a Specific Need?

[81] While not specific to BWCs, OIPC's Guidance document on *Video Surveillance by Public Bodies in Newfoundland and Labrador* suggests a first step is to determine: "[i]s there a real, pressing and substantial problem which is ongoing in nature that has not and cannot be mitigated by other less privacy intrusive measures?" As this has been discussed in detail in the Authority for Collection section above, we will not repeat it here. The Town has not provided the information necessary for OIPC to determine that the program is, in fact, necessary.

Is it Likely to be Effective in Meeting that Need?

[82] The Town discussed the importance of having the "assurance of good and honest conduct by its officers, and public confidence in those officers." In discussing the importance and benefit of objective evidence, especially when faced with a "he said/she said" situation, the Town quotes from *R. v Caines*:

> *Sometimes, cameras make better witnesses than humans. In trial matters, they can be invaluable in ensuring that accurate and reliable evidence is presented through their recordings of events. They are incapable of convincing themselves that they saw something that did not occur.*

[83] This case details allegations that the accused was using a cell phone while driving, which would be a violation of the *Highway Traffic Act*. This is an interesting case to cite in support of cameras, as the video did not capture the information necessary to verify the accounts of either party involved. The above quote is at paragraph 1; paragraphs 12 and 27 discuss what was captured on the recording:

> *[12] The video recorded is clear and of excellent quality. It shows the police vehicle Sergeant Foster was operating drive up the exit lane and stop at the stop sign. It shows Ms. Caines' vehicle pass by the police vehicle. It passes by quickly and it is impossible to see anything inside her vehicle.*
> ...
> *[27] As noted earlier, the video was of an excellent quality. I am satisfied that I can rely upon it. It clearly shows Ms. Caines' vehicle being driven past the police vehicle being operated by Sergeant Foster. There are two things that stand out: (1) Sergeant Foster had little time to observe what Ms. Caines was doing; and (2) the video does not show anything inside Ms. Caines' vehicle.*

[84] In this case, the Judge decided that indeed, the video was conclusive evidence, but conclusive only in demonstrating what the cameras could not see; the video recording did not provide the information necessary to support the account of either individual. It is possible that the BWC program will not provide the Town with the information it is seeking. Although OIPC asked the Town for specific examples and further details on how the BWC program will address the issues being experienced by the Town, the Town's submission did not provide the requested details.

Is the Loss of Privacy Proportional to the Need?

[85] When examining if the loss of privacy is proportional to the need, the Town's first submission focused on what was being done to protect information once it was collected, noting in part:

> *Where the loss of privacy comes into question it is proportional as there is protection concerning the data access utilizing the latest Redaction software to protect and indirect privacy breaches should the data collected be needed for an investigation and court purpose.*

[86] This discussion does not establish a need for this new initiative; rather it focuses on the steps that the Town is taking to protect the personal information once it is collected. Further, although the submission mentioned using the "latest redaction software", the second submission confirmed that the Town has not yet procured such software. Our recent experiences, detailed in Report A-2021-014, have revealed that the post-facto procurement of video redaction software may not be as simple as the Town seems to believe. BWCs have the capability to capture the images, actions and conversations of individuals not directly involved in the incident; they also go wherever the MEO or ACO goes, which could possibly

include private dwellings. Although OIPC inquired about any restrictions on when video would be recorded, no additional information was provided.

[87] The loss of privacy that must be addressed is the loss associated with the operation of the program itself, including all of the identifying images of citizens collected by the BWC. That loss of privacy must be weighed against the identified need, to determine whether the need is indeed of sufficient weight to warrant the routine collection of personal information without consent through the BWC.

Is there a Less Privacy-Invasive Way of Achieving the Same End?

[88] When the initiative was initially brought to Town management for discussion by the MEO in June 2019, the MEO noted that he carries out his duties alone, without a partner to help or corroborate his recall of interactions, and he relied on the back-up of the RCMP if needed and available. " [the MEO] also advised that throughout the course of his daily duties he had encountered many situations whereby members of the public had made claims on social media indicating that he had acted either unprofessionally or outside the scope of the Municipal Enforcement Department mandate." The MEO indicates that there is a culture of mistrust of Town law enforcement.

[89] While the Town's second submission indicates that Management looked at its options to address this matter, no additional information is provided about those options. The second submission comments:

> *Perhaps most importantly, the Town sees a total lack of alternatives to effectively address the issues it faces with its law enforcement program. Objective records of interactions are the Town's best option, and any resulting invasion of privacy would be outweighed by the program's benefits.*

[90] While it is a positive step that the Town recognizes the trade off between an individual's privacy and the benefits of the program, based on the information provided, OIPC is not convinced that there is a need for the program or that BWCs will address the issues the Town is facing. Further, it does not appear that the Town has taken any other steps to address these issues. For example, it is unclear how BWCs will build trust in municipal enforcement officers

or stop social media comments by residents, unless the Town expects to post its own videos of incidents to social media sites, which is not recommended.

[91] As part of this investigation, OIPC requested records relating to the decision to purchase BWCs. This is a privacy invasive technology that would normally require extensive review and consideration. In its second submission, the Town confirmed that approval to purchase the BWCs was not required from Council; however, the policy to use them did require approval of Council. It is concerning that no documentation exists supporting the decision to purchase and use this privacy invasive technology, and only minimal consideration of legislative requirements. This suggests a complete lack of a Privacy Management Program within the Town.

[92] The Town needs to ensure that it understands how applicable laws, including *ATIPPA, 2015*, impact its programs and decisions. There was very limited evidence provided to OIPC during this investigation to conclude that the Town's BWCs program was deployed in a manner that properly considers, respects, and protects the general public's and employees' right to privacy.

IV DECISION

[93] A BWC program has the potential to capture a lot of personal information. Further, it has the potential to collect more information than needed for the identified purpose. It captures both audio and video. It may collect information about bystanders or individuals passing near the scene. If the incident is occurring in a private dwelling, it could record exceptionally private areas.

[94] The Town's BWC program has been done precisely backward. A member of staff seems to have identified an issue – unproven allegations that were being made against him and a lack of trust in Town law enforcement (i.e., him) – and proposed a solution: BWCs. Generally speaking, as appreciated by the Supreme Court of Canada in *R v Oakes,* but well known to policy professionals everywhere, the policy process should work the other way around: a policy problem is identified and then research is done into multiple solutions, the comparative

advantages and disadvantages of each of which are weighed prior to taking action. There appears to be little doubt that there is a trust issue between segments of the population and Town officials, in particular the MEO, as demonstrated by the recent incident that was captured on video and the subsequent social-media fueled controversy. But the immediate leap to conclude that the only possible solution to restoring the trust of this population is through largely indiscriminately collecting their personal information is not logical. If trust is the problem, there are numerous other actions that could be explored; first among them, community engagement. The Town provided no evidence that this approach was explored to address the Town's policy problem, but there was also no community engagement about the solution that it immediately jumped to. Even if trust were not a problem before, commencing with a broad and indiscriminate collection of personal information without community engagement is sure to make it a problem. The backwardness of the Town's approach to the policy process is further illustrated by the lack of any evidence that Council even considered the policy problem. To be more precise, BWCs were discussed, but there is no indication that Council grappled with the underlying problem of a lack of trust in Town enforcement. Leaping directly to one pre-selected solution is probably the most common and fatal flaw found in policy development at all levels of government.

[95] There is a further critical step that the Town seems to have missed. The Town, like any public body or public official that works for it, can only exercise its authority on the basis of law. There needs to be a legal basis for its expenditure of funds or any other regulatory actions that it takes. In particular, the Town needs to have a clear legal basis for the collection, use, storage and disclosure of personal information. The Town appears to have decided to collect, and indeed commenced collecting using and disclosing, personal information without analyzing in advance what authority that it had to do so. As above, it decided what it wanted to do and went looking for the legal authority after the fact, once questioned about it. Even at this date, the Town still appears to be unclear about whether its Municipal Enforcement Officer is a peace officer or rather, per the *Municipalities Act, 1999*, has the powers of a police officer for certain purposes. The notion that the Town has officials in the community exercising law enforcement authorities when it is unclear whether they have those authorities has implications for how they collect personal information, but beyond that, is quite troubling in general.

[96] As noted, BWCs are a highly privacy invasive tool used by law enforcement. We do not deny that there may be a place for them. They are ubiquitous in the United States and increasing in use in Canada. There are numerous studies about their effects which examine whether they do what they are purported to do, i.e. increase transparency and accountability for law enforcement. This report is not intended to be a guidance document on their use and has already cited such a document developed in 2015 that is still relevant. However, it is worth reiterating that Canadian Commissioners have concluded that, while there may be specific situations that justify the use of BWCs, they should only be implemented where the public policy imperative balances against the privacy invasiveness. It is hard to believe, that of all places in Newfoundland and Labrador, the Town of Happy Valley-Goose Bay is the one place where BWCs are justified. Commissioners further declared, as is required by *ATIPPA, 2015*, that the appropriate safeguards be put in place. The Town initiated the BWC program without completing the process of putting those safeguards in place. Many jurisdictions in Canada which have implemented BWCs have done so following extensive research and consultation with the community and parties such as Information and Privacy Commissioners, the provincial government, and Human Rights Commissioners. The Town has done none of this.

[97] We must also comment on the Town's cooperation with this Office prior to and during this investigation. As described above, this Office learned of this initiative through the media and made numerous inquiries to the Town. Requests for information to Town officials would commonly go unanswered for weeks and months at a time. It was for this reason, as well as a questioning about the authorities of the OIPC, that a formal investigation was launched in December 2020 with the intent to give a clear legal framework to our investigation. Even still, the Town was delayed in responding to our requests for information. At the time of writing, the Mayor has not directly responded to our January 2021 letter to him about this subject, though the Town did ultimately and belatedly provide much of the information we requested.

[98] One challenge that the Town has faced during this period has been turnover. The Town, on paper, seems to be amply resourced to discharge its mandate; however, it seems to have had, at least during this period, a considerable problem with staff turnover. Numerous key positions were vacant for extended period during this time. While this problem caused

difficulties for our investigations, it is also relevant for the matter of a BWC program. The design and implementation of a legally compliant BWC program is complicated. Many things about it require work by the officers themselves and other officials who need to provide oversight. We have significant doubts whether the Town, even fully staffed, has the capacity to properly design and implement such a program. This may help explain why it is difficult to find a Town of a comparable size – in this province or elsewhere in Canada – with such a program.

[99] The Town's submission emphasizes that the BWC program is on hold and that further changes to the program are expected before resumption:

> *The OIPC's compliance assessment and ensuing report should take into account the fact that the BWC program has been on hold since October 2020, and that updates to the BWC Program have not yet been finalized and approved by Council. There will be important changes to the program that was put in place earlier in 2020, and the Town looks forward to the OIPC's input and recommendations.*

The Town intends to restart the program once it has, "a robust 'best practices' policy and sound procedures in place to guide the program." While this OIPC investigation is one of the reasons that the program remains on hold, the second submission also notes that the "primary reason is because the Town needs to get this program right."

[100] The Town's BWC policy and program are not compliant with *ATIPPA, 2015*. The Town should formally suspend its BWC program immediately. Notwithstanding that the program is "on hold", the Town should provide certainty by formally suspending the program through a motion of Council. We are of the view that the Town should consider entirely abandoning the initiative and re-examine its approach to the policy problem – trust issues with Town enforcement – from scratch; however, we recommend that it should, at a minimum, overhaul its policy through conducting appropriate consultation and addressing the deficiencies identified in this report, taking the steps detailed in the recommendations below.

[101] This Report examines the requirements of Part III of *ATIPPA, 2015* and any initiative that collects, uses or discloses personal information must be in compliance with all applicable

sections of the *Act*, including authority to collect, use and disclose; establishing reasonable safeguards; and ensuring appropriate privacy notices are in place. Based on the information provided to OIPC during the course of this investigation, there are significant deficiencies in the Town's compliance with the law.

[102] While the Town has put its BWC program on hold, concerns remain that the Town collected information through this program from July 2020 to November 2020.

V RECOMMENDATIONS

[103] Under the authority of section 76(1), I recommend that the Town stop collecting, using or disclosing personal information using BWCs until such time that it can demonstrate full compliance with *ATIPPA, 2015.* This Report provides considerations for amassing the required information and the necessary analyses should it wish to recommence the program. Further, I recommend that any information already collected by this program be held securely with no access to anyone except as required in the course of a legal proceeding.

[104] Under the authority of section 76(2), I recommend that the Town develop a privacy management program. Approvals of such privacy invasive initiatives should require high level oversight within the public body. As this was a low cost purchase, there was only the need for approval by the Department head. While the cost may have been low, the potential impact is high. The Town must ensure the appropriate processes are in place to review and approve initiatives with significant privacy implications. Further, any such program should also include mechanisms to periodically review programs.

[105] It is clear through the Town's submission that it intends to relaunch its BWC program. Prior to re-starting the program, I recommend under the authority of section 76(2) that the Town:

- Conduct a robust privacy assessment of the program and submit to OIPC for review prior to program launch.
- Update the BWC policy to ensure compliance with *ATIPPA, 2015*, including mechanisms to ensure adherence with the policy.

- Conduct public consultation regarding the proposed program, including discussions of the impact the program will have on individual privacy.
- Develop and execute a plan for communicating about the program with the public, notifying them about the program and who they can contact if they have questions or concerns.
- Obtain appropriate redaction software and ensure training is conducted or identify a service that can be contracted on as needed basis that is sure to work, to ensure prompt and fair processing of access requests, be they formal or informal.

[106] As set out in section 78(1)(b) of *ATIPPA, 2015*, the head of the Town of Happy Valley-Goose Bay 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.

[107] Dated at St. John's, in the Province of Newfoundland and Labrador, this 4th day of May 2021.

Michael Harvey
Information and Privacy Commissioner
Newfoundland and Labrador