Guidance for Public Bodies on the Use of Video Surveillance

Table of Contents

Acknowledgements

These guidelines draw upon information contained in video surveillance guides from Service Alberta, the Office of the Saskatchewan Information and Privacy Commissioner, the Office of the Information and Privacy Commissioner, Ontario, and the Office of the Privacy Commissioner of Canada. That contribution is gratefully acknowledged.

Purpose

The purpose of these guidelines is to assist public bodies identify when it is appropriate to use video surveillance and evaluate whether in using video surveillance involving the collection, use and disclosure of personal information the requirements of the *Access to Information and Protection of Privacy Act* (ATIPP Act) can be met.

Definitions

Covert video surveillance means the secretive, continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals that is recorded using video surveillance.[1]

Law enforcement is as defined in section 3 of the ATIPP Act (see page 7 of these guidelines for the meaning).

Personal information is as defined in section 3 of the ATIPP Act (see page 4 of these guidelines for the meaning).

Record is as defined in section 3 of the ATIPP Act and includes *"books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other process or mechanism that produces records;*"

Video Surveillance refers to a mechanical digital, electronic or wireless surveillance system that enables periodic or constant video recording, observing or monitoring of personal information about individuals.

[1] *Video Surveillance: The Privacy Implications*, IPC Practices, Number 10, September 1998, Ontario Information and Privacy Commissioner's Office citing guidelines produced in 1992 by the Privacy Commissioner of Australia, pg.1.

Scope and Explanatory Notes

This guidance is limited to video surveillance that results in the recording of "personal information" which is defined in section 3 of the *Access to Information and Protection of Privacy Act* (ATIPP Act) as "recorded information about an identifiable individual". The recorded image, personal characteristics, voice, speech and mannerisms of an individual are considered to be personal information if that individual can be identified from the record.[2]

These guidelines identify seven steps designed to assist a public body decide whether to implement a video surveillance system that records personal information and whether in doing so it will meet the requirements of the ATIPP Act.

This guidance does not apply to covert video surveillance which may occur as part of recording personal information for law enforcement purposes. A public body that is considering using video surveillance covertly should consult with legal counsel to ensure compliance with any applicable laws, including the ATIPP Act.

This guidance was prepared to help public bodies meet the requirements of the ATIPP Act. It is not intended, nor is it a substitute for legal advice. For the exact wording and interpretation of the ATIPP Act, please read the ATIPP Act in its entirety. This document is not binding on the Yukon Information and Privacy Commissioner.

All section references in these guidelines refer to the ATIPP Act unless otherwise stated.

[2] *Ibid.*

Preliminary Considerations

Step One: Before deciding to use video surveillance, a public body should consider whether there are less privacy intrusive means to collect personal information.

Video surveillance systems are being employed with more and more frequency throughout Canada as well as in the Yukon. Although used for many purposes, the common use of video surveillance is to detect and deter crime. While video surveillance may be effective at detecting and deterring crime, video surveillance captures much more than just criminal activity, it also captures citizens going about their daily activities. Recording such activities makes video surveillance very privacy intrusive. Because of this, the implementation standards for video surveillance are much greater than those of other surveillance systems.

A public body should consider the following before reaching a decision to use video surveillance:

- Evaluate the reasons for considering the use of video surveillance. Cost saving or ease of use is not reason enough to use video surveillance over other forms of surveillance, such as foot patrols. Only after other less privacy intrusive means of surveillance have been considered and determined unworkable and it has been determined that there is a compelling need to use video surveillance should it be considered as an option.

- Carefully weigh the benefits to be gained from using video surveillance against the invasion of privacy on those individuals whose personal information will be recorded by the video surveillance. A decision to use video surveillance should only be arrived at after a public body determines that the benefits to be gained from the use of video significantly outweigh the loss of privacy that will result.

- Consider the sensitivity of the personal information to be collected using video surveillance. The higher the sensitivity, the more difficult it will be for the benefits to outweigh the risks to privacy.

Once a public body satisfies itself that the use of video surveillance is warranted in the circumstances, it then needs to determine if the collection, use and disclosure of the personal information collected via the video surveillance is in compliance with the ATIPP Act.

See page 18 for an Example of this step.

Complying with the ATIPP Act

Step Two: Before collecting personal information by video surveillance, a public body needs to determine whether it has authority under the ATIPP Act to do so.

Public bodies are required to meet the requirements of sections 29 and 30 in Part 3 for the collection of personal information.

Section 29 of Part 3 states:

> *No personal information may be collected by or for a public body unless*
>
> > *(a) the collection of that information is authorized by an Act of Parliament or of the Legislature;*
> >
> > *(b) that information is collected for the purposes of law enforcement; or*
> >
> > *(c) that information relates to and is necessary for carrying out a program or activity of the public body.*

Section 29 means that a public body must not collect, use or disclose personal information, including by video surveillance, unless the collection, use or disclosure is for one or more of the purposes identified in this section.

Does paragraph 29 (a) apply?

> *29 No personal information may be collected by or for a public body unless*
> *(a) the collection of that information is authorized by an Act of Parliament or of the Legislature;*

In order to rely on paragraph 29 (a), a public body must be able to identify an Act of Parliament of Canada or of the Legislature that authorizes it to collect the personal information it is seeking to collect by video surveillance. In the *Yukon Interpretation Act*, "Act" is defined as "*an ordinance of the Yukon enacted pursuant to the Yukon Act (Canada)*."

Does paragraph 29 (b) apply?

> *29 No personal information may be collected by or for a public body unless*
> *(b) that information is collected for the purposes of law enforcement;*

"Law enforcement" is defined in section 3 as:

> *(a) policing, including criminal intelligence operations,*
>
> *(b) investigations that lead or could lead to a penalty or punishment being imposed or an order being made under an Act of Parliament or of the Legislature,*
>
> *(c) proceedings that lead or could lead to a penalty or punishment being imposed or an order being made under an Act of Parliament or of the Legislature, and*
>
> *(d) investigations and proceedings taken or powers exercised for the purpose of requiring or enforcing compliance with the law;*

In order for a public body to collect personal information for the purposes of law enforcement under subsection 29 (b), it will have to satisfy itself that the collection of personal information is for one of the purposes listed in paragraphs 3 (a) through (d) of the definition of law enforcement.

Does paragraph 29 (c) apply?

> *29 No personal information may be collected by or for a public body unless*
>
> *(c) that information relates to and is necessary for carrying out a program or activity of the public body.*

If a public body seeks to rely on paragraph 29 (c), collection for the purposes of carrying out program or activity, for the use of video surveillance it must satisfy itself that the collection of personal information using video surveillance "is related to a legitimate operating program or activity of the public body" and that the personal information to be collected is "necessary" for the purpose identified.

Use of the word "necessary" in paragraph 29 (c) indicates that a public body must **limit** the personal information collected only to that which is needed. Necessary does not mean indispensable, however, personal information that would be merely helpful to carrying out the activity or program is not necessary.[3]

In order to determine whether it can meet the requirement to limit the personal information collected to that which is necessary, a public body should:

1. Examine in detail each piece or category of personal information to be collected and the reason for collecting it.

[3] Order F07-10 Board of Education School District No. 75 (Mission) June26, 2007 at para. 49 (BC IPC).

2. Determine exactly which personal information is required in order to properly administer the program or activity the public body is carrying on. In making this determination consider the sensitivity of the personal information, the particular purpose for the collection, and the amount of personal information collected in light of the purpose for collection.

Collecting personal information through video surveillance presents some unique challenges for public bodies in meeting the requirement to limit the collection of personal information to that which is necessary. The amount of personal information that may be recorded through video surveillance may result in the collection of more personal information than is necessary. There are a number of things a public body can do to limit the amount of personal information collected through video surveillance. A public body can ensure that the area captured by video surveillance is restricted as much as possible to the area of concern. It can also restrict use of the camera to hours where the risk or need associated with the purpose of collection is highest.

See page 19 for an Example of this step.

Step Three: Before collecting personal information by video surveillance, a public body also needs to determine whether it is required to provide notice about the collection.

Subsection 30 (2) of the ATIPP Act states that:

> *A public body must 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.*

Subsection 30 (2) is considered the "notice" provision. This provision requires that notice be given for any collection of personal information by a public body unless one of the two exceptions contained in subsection 30 (3) to this requirement applies. They are:

> *(a) the information is about law enforcement or anything referred to in section 19;*
>
> *or*

(b) the Minister responsible for this Act excuses the public body from complying with it because compliance would

(i) result in the collection of inaccurate information, or

(ii) defeat the purpose or prejudice the use for which the information is collected.

There are no specific requirements set out in section 30 (2) as to when or how notice is to be given. In the context of video surveillance it is a best practice to provide individuals with notice prior to their entering the area under video surveillance to give them the option not to have their personal information recorded. To facilitate this choice, notice about the collection of personal information by video surveillance should be placed in an area most likely to be seen by individuals prior to entering the area under video surveillance. As well, notices posted should be understandable and written in simple language and it should be clear from the notice what area is under video surveillance.

See page 20 for an Example of this step.

Step Four: Before <u>using personal information</u> collected by video surveillance, a public body needs to determine whether it has authority under the ATIPP Act to do so.

The ATIPP Act limits the use of any personal information collected. Subsection 35 (1) states that a public body many only use personal information collected:

(a) for a purpose for which that information was obtained or compiled or for a use consistent with that purpose;

(b) if the individual the information is about has consented to the use; or

(c) for the purpose for which that information may be disclosed to that public body under section 36 to 39.

Subsection 35 (2) states that *"a public body may use personal information only to the extent necessary to enable the public body to carry out its purpose in a reasonable manner."*

Section 37 states that a use will only be consistent with the purpose of collection where use of the personal information:

(a) has a reasonable and direct connection to that purpose; and

(b) is necessary for performing the statutory duties of, or for operating a legally

authorized program of, the public body that uses the information or to which the information is disclosed.

Where a public body is collecting personal information using video surveillance, its use of that personal information will generally be limited to those circumstances described in paragraph 35 (1) (a). To meet the requirements of this paragraph, a public body must ensure that any use of the personal information collected using video surveillance is used only for the purpose it was collected or for a use consistent with that purpose.

In order to determine if a use is for a consistent purpose, a public body must be able to establish that the proposed use has a reasonable and direct connection to the purpose of collection. A public body must also establish that the information to be used is necessary to achieve the purpose identified. Necessary does not mean indispensable, however, personal information that would be merely helpful to carrying out the activity or program is not necessary.[4]

In order to meet the requirement in subsection 35 (2), a public body must limit its use of the personal information only to the purpose identified. Any use of the personal information beyond this purpose will be contrary to the ATIPP Act.

See page 20 for an Example of this step.

Step Five – Before disclosing personal information collected by video surveillance, a public body needs to determine whether it has authority to do so.

The only circumstances under which a public body may disclose personal information are set out in section 36. These circumstances are as follows:

(a) in accordance with Part 2;

(b) if the individual the information is about has consented, in the prescribed manner, to its disclosure;

(c) for the purpose for which it was obtained or compiled or for a use consistent with that purpose;

(d) for the purpose of complying with an enactment of, or with a treaty, arrangement or agreement made under an enactment of Canada or the Yukon;

[4] *Ibid.*

(e) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information;

(f) to an officer or employee of the public body or to a Minister, if the information is necessary for the performance of the duties of the officer, employee or Minister;

(g) to the legal counsel for the Government of the Yukon or its insurers for use in civil proceedings involving the Government;

(h) for the purposes of the Coroners Act, or the Public Guardian and Trustee's functions under the Public Guardian and Trustee Act;

(i) for the purpose of

(i) collecting a debt owing by an individual to the Government of the Yukon or to a public body, or

(ii) making a payment owing by the Government of the Yukon or by a public body to an individual;

(j) to the auditor general or any other prescribed person or body for audit purposes;

(k) to the Yukon Archives;

(l) to a public body or a law enforcement agency in Canada to assist in an investigation

(i) undertaken with a view to a law enforcement proceeding, or

(ii) from which a law enforcement proceeding is likely to result;

(m) if the public body is a law enforcement agency and the information is disclosed

(i) to another law enforcement agency in Canada, or

(ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;

(n) if the public body determines that compelling circumstances exist that affect anyone's health or safety and if notice of disclosure is mailed to the last known address of the individual the information is about;

(o) so that the next of kin or a friend of an injured, ill, or deceased individual may be contacted; or

(p) in accordance with section 38 or 39.

Prior to disclosing any personal information collected by video surveillance, a public body must satisfy itself that the disclosure is for one of those circumstances listed in section 36.

A public body may need to revisit section 36 from time to time to determine whether it has authority to disclose personal information collected by video surveillance. A public body, should, however, identify any anticipated disclosures of this information before collecting it as a means to provide guidance to its employees on authorized disclosures under the ATIPP Act.

See page 21 for an Example of this step.

Step Six – Before collecting personal information by video surveillance, a public body needs to determine how it will secure and retain the personal information collected.

Section 33 states:

> *33 The public body must protect personal information by making reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal.*

Public bodies must have administrative, technical, and physical controls in place in order to meet the requirement of section 33.

Administrative controls are policies and procedures established by a public body that set out the rules required to protect personal information, including with respect to the collection, use, disclosure, access, storage, retention and destruction of personal information. Technical controls are electronic controls used to protect personal information. Physical controls are environmental controls, such as locked doors or security systems, used to protect personal information.

In order to determine what a "reasonable security arrangement" is as it relates to the protection of personal information, a public body needs to evaluate the sensitivity of the personal information. Information that is highly sensitive will require more security than information that is considered low or moderately sensitivity.

While a public body can, to a certain degree, anticipate the type of personal information that will be collected through video surveillance, it may find that the information recorded is much more sensitive than originally anticipated. This uncertainty about what will be collected through video surveillance indicates the need to have strong security in place to properly protect the personal information recorded using video surveillance. Examples of security a public body might employ for video surveillance records are as follows:

1. Video surveillance recordings should be stored in a location with restricted access and logs maintained of any access.

2. Digital video recordings need to have proper technical controls in place to prevent unauthorized access to the recording.

3. Access to the records should be limited to employees who require access to the content of the recordings as part of their job duties. The identity of these employees should be clearly specified.

4. Employees with access to the recordings should receive privacy training specific to their duties. Privacy training should be completed prior to providing access to the recordings.

5. A process for viewing the recordings should be established. This process should include the circumstances under which a recording can be viewed and a requirement that viewing should not occur unless senior management authorizes the viewing.

6. A log should be kept any time a recording is viewed including for access to digital video recordings. For audit purposes, these logs should include the identity of the employee who viewed the recording, the reason for viewing, the date and time of viewing, and the purpose of any subsequent uses or disclosure of personal information in the recordings. For access to digital recordings stored electronically, the system should be capable of capturing data about who accessed the recording, when and for what time period. This capability should be activated.

7. For any disclosures of personal information contained in the recordings, a log should be kept indicating the identity of the employee who disclosed the personal information, what personal information was disclosed, who the personal information was disclosed to, the purpose of the disclosure, and the date and time of the disclosure.

8. Clear rules about what is to occur in the event of a security breach should be specified.

Section 34 of the ATIPP Act requires a public body to retain a record for at least one year if the record is used to make a decision that directly affects an individual to allow the individual who is the subject of the personal information the opportunity to obtain access to it. An example of when a public body would be required to retain a record is where a public body decides to disclose to a law enforcement agency a video recording that captures an individual engaging in a crime. The decision to disclose the video recording to the law enforcement agency would likely be considered a decision by the public body that directly affects this individual.

Some best practices with respect to the retention of video surveillance records are as follows:

1. For non-viewed recordings, the recording should be retained only as long as is needed and erased as soon as they are no longer needed. Taking into account any legal considerations, the public body should clearly define how long non-viewed recordings are to be kept and when they are to be erased or over written.

2. For viewed recordings, the recording should be retained as long as they are required to meet any legal or business needs. Where a decision is made that directly affects an individual, the recording should be retained for at least one year to allow the individual to request access to it.

3. Recordings that do not need to be retained or which period of retention has expired should be securely destroyed or deleted. Deletion or destruction of the recordings should occur in such a way that the personal information on the recordings cannot be retrieved or restored. Examples of ways to securely destroy recordings include overwriting electronic records, shredding, burning or magnetically erasing them.

See pages 21 and 22 for an Example of this step.

Step Seven: Before collecting personal information by video surveillance, a public body needs to determine how it will accommodate requests for access to a video surveillance record.

Another important consideration that a public body will want to take into account when considering technology associated with video surveillance is how it will meet its obligation to provide access to video surveillance records under Part 2.

An issue that arises from time to time with respect to requests for access to video records is a claim by a public body that access to a video record cannot be accommodated. The reason often cited in these requests, is that the public body has no ability to redact from the video record third party personal information found by the public body to constitute an unreasonable invasion of the third party's personal privacy. In order to accommodate an individual's right of access under subsections 5 (1) and (2), a public body will need to ensure it has the technology to redact personal information from a video recording as needed in order to accommodate a right of access.

See page 23 for an Example of this step.

Developing a Video Surveillance Policy

Policies and procedures developed by a public body should clearly specify the rules employees must follow for the collection, use, disclosure, security and retention of personal information collected by video surveillance. At minimum these policies and procedures should contain the following:

1. Circumstances under which it is acceptable to use video surveillance. These circumstances should include a requirement to limit the use of video surveillance to circumstances where:

    a. other forms of surveillance have been tried and failed or are not feasible in the circumstances (cost should not be the only factor considered),

    b. there is a compelling need to use video surveillance,

    c. the benefits to be derived from using video surveillance significantly outweigh the loss of privacy that will result, and

    d. the sensitivity of personal information to be collected using the video surveillance has been considered in weighing the benefits against the risks.

2. The rules that must be followed when collecting, using and disclosing personal information using video surveillance to ensure the requirements of the ATIPP Act are met. These rules should include a requirement to ensure:

    a. the purpose of collecting the personal information is clearly identified and documented,

    b. there is authority to collect the personal information and the personal information collected:

        i. is limited to only that personal information necessary for the purpose identified and that the sensitivity and amount of personal information is considered in limiting collection, and

        ii. the location and positioning of the surveillance cameras as well as the timing and duration of the video surveillance are considered to prevent over collection,

    c. notice is provided to individuals where required and the requirements for giving proper notice are specified,

d. the uses of the personal information collected are identified, there is authority to use this personal information under the ATIPP Act, the use is limited to what is necessary to achieve the purpose, and the personal information is only used for the purpose identified,

e. anticipated disclosures of personal information collected are identified, there is authority to disclose the personal information under the ATIPP Act, and disclosure is limited to the information required to meet the purpose of disclosure,

f. the personal information collected is properly secured and retained, including specific rules about:

    i. the need to evaluate the level of sensitivity as part of determining the level of security required,

    ii. where the personal information will be stored and under what conditions,

    iii. when a privacy impact assessment and security threat risk assessment should be undertaken,

    iv. who will have access to the personal information and how this access will be managed,

    v. when recordings will be viewed and under what circumstances,

    vi. the need to maintain viewing logs and what these logs must contain,

    vii. how and when the logs will be audited to ensure compliance,

    viii. how long the recordings and logs will be retained including when there is a request for access to the personal information,

    ix. how requests for access to the personal information will be managed, and

    x. what will occur in the event of a breach of security.

3. A requirement that video surveillance records are able to be redacted in order to facilitate requests for access to information.

4. A requirement that a senior employee is designated as responsible for each video surveillance system and accountable for compliance with the policies and procedures.

5. A requirement that all employees and contractors receive privacy training specific to the video surveillance policies and procedures and their duties thereunder.

6. A requirement that employees sign agreements indicating they have read and understand their responsibility to follow the policies and procedures and that they have had privacy training in relation to these responsibilities.

7. A statement indicating that employees will be subject to discipline if they breach the policies and procedures.

8. A requirement that any contracts entered into where the contractor will have access to the personal information specify:

    a. that control of the personal information collected using video surveillance will remain with the public body,

    b. that contractors must comply with the public body's video surveillance policies and procedures,

    c. that contractors must participate in training on their responsibilities with respect to these policies and procedures,

    d. that contractors will ensure their employees receive privacy training to ensure compliance with these policies and procedures and have them sign confidentiality agreements acceptable to the public body,

    e. the process for managing a breach of security and requests for access to personal information,

    f. what will occur in the event a contractor violates the policy and procedures, and

    g. the ability to audit the contractor to ensure compliance with the policies and procedures.

9. A requirement that all video surveillance policies and procedures are reviewed and updated at least every two years or sooner if required and that training is updated when revisions are made.

Examples

Step One Examples

AAA is a public body subject to the ATIPP Act. AAA has an employee parking lot located at the rear of its building. For a period of four months, employees reported car break-ins during their evening shift. During this same period employees also reported suspicious looking individuals in the parking lot at night when returning to their car following their evening shift. These employees indicated they feared for their safety.

AAA recognized a need to take action to ensure its employees that use the parking lot are safe. AAA examined its options and, recognizing the privacy invasive nature of video surveillance, it decided to implement foot patrols in the parking lot. It also installed fencing around the parking lot. After several months passed and the reports of crimes and suspicious characters continued, it considered whether it should also use video surveillance.

Before deciding to use video surveillance, AAA considered the benefits to be gained by using video surveillance against the risks to individual privacy. It identified there would be significant benefits to be gained by using video surveillance. Specifically, that continuous monitoring will increase the safety and security of employees who use the parking lot by increasing the ability to capture crimes occurring and deterring these crimes. It identified the risks to individual privacy as moderate recognizing that the personal information recorded would be images and activities of individuals who enter a parking lot.

On balance, given the evidence of criminal activity in the parking lot together with the benefits to be gained through use of video surveillance in comparison to the loss of privacy that would result, AAA decided it was reasonable to use video surveillance in the employee parking lot.

After completing Step One, AAA moved on to step two.

BBB is a public body that is subject to the ATIPP Act. BBB has an employee parking lot located at the rear of its building. After hearing about what was occurring in AAA's employee parking lot, it considered using video surveillance to prevent crime from occurring in its employee parking lot. BBB is located across town from AAA and has received no reports of crime in its employee parking lot.

In order to make a decision about whether to use video surveillance, after determining another form of surveillance was not feasible, BBB considered the benefits to be gained by using video surveillance against the risks to individual privacy. It identified the risks to individual privacy as being moderate recognizing that the personal information recorded would be images and activities of individuals who enter a public parking lot.

On balance, BBB determined that because it had received no reports of crime or potential crime occurring in the employee parking lot the risks to individual privacy are not outweighed by the benefits to be gained through use of video surveillance. As a result, BBB decided it would not use video surveillance and, therefore, no further steps were needed.

Step Two Example

After completing step one, AAA went on to step two to determine whether it has authority under the ATIPP Act to collect the personal information by video surveillance.

AAA conducts and assessment to determine if it has authority under section 29 to collect the personal information that will be captured through video surveillance of its employee parking lot.

First, it identifies that its purpose of collecting the personal information is to provide a safe and secure parking lot for its employees by detecting and deterring crime in the parking lot.

Second, it examines if this purpose meets any of the purposes listed under section 29. It determines that paragraph 29 (a) does not provide authority as there is no Act of the Parliament of Canada or the Yukon Legislature that authorizes it to collect the personal information. It determines that paragraph 29 (b) does not provide authority as its purpose of collecting the personal information is not for policing, an investigation or a proceeding. It then looks at paragraph 29 (c) for authority. In looking at its program and activities, it determines that as an employer one of its activities is to provide a safe work environment for its employees. Ensuring the parking lot is safe for employees is part of this activity and collection of the personal information through video surveillance is related to this activity. AAA determines it has met the first requirement of subsection 29 (c) that the personal information to be collected is related to a legitimate operating program or activity of the public body.

Next, it examines if the personal information it will collect is necessary. It identifies it will collect the images and activities of individuals entering the employee parking lot which is accessible by the public. It determines the sensitivity of this personal information as moderate. It then assesses what personal information it needs for the purpose of carrying on the activity of providing a safe and secure parking lot for its employees by detecting and deterring crime in the parking lot. It determines that collection of the images and activities of individuals entering the parking lot is necessary in order to carry out the activity but that the collection of images and activities of individuals beyond the parking lot is not necessary.

To limit collecting images and activities of individuals beyond the parking lot, AAA explores ways it can limit the personal information collected using video surveillance. It retains an expert to discuss options. It explains to the expert that the video camera needs to capture the entire employee parking lot but nothing beyond the parking lot. It further identifies the need to limit recording to between the hours of 8:00 PM and 12:00 AM based on the reports received from employees all who indicated that the criminal activity was occurring between these hours. The expert assists AAA choose the camera with the range needed, identify the areas to install the cameras to limit filming only the parking lot, and how to set the timers to film only during the hours indicated.

After completing step two, AAA moved on to step three.

Step Three Example

After completing step two, AAA went on to step three to determine whether it is required to give notice to collect personal information using video surveillance.

It determined it was required to provide notice about the collection of the personal information using video surveillance in its parking lot. It then prepared a sign containing the following to meet the requirements under subsection 30 (2) and in accordance with best practices.

WARNING - EMPLOYEE PARKING LOT UNDER VIDEO SURVIELLANCE

AAA is collecting video images of persons entering this parking lot for the purpose of employee safety and security by detecting and deterring criminal activity.

AAA is authorized by paragraph 29 (c) of the Access to Information and Protection of Privacy Act (ATIPP Act) to collect this personal information as the collection relates to and is necessary for a program or activity of AAA.

The collection, use and disclosure of this personal information is being conducted in accordance with the ATIPP Act.

If you have any questions about the collection of this personal information, please contact AAA's ATIPP Coordinator at 123 Any Street, 667-0000, atippcoordinator@gov.yk.ca

AAA posted this sign at all the entrances to the parking lot and in various places located within the parking lot. It also placed an announcement about the surveillance in the employee newsletter two weeks prior to the start of the video surveillance indicating the date on which the video cameras would be turned on and who to contact for more information.

After completing step three, AAA moved on to step four.

Step Four Example

After completing step three, AAA went on to step four to determine whether it has authority to use the personal information collecting using video surveillance.

After determining that paragraphs 35 (1)(b) and (c) did not apply, it considered whether it met the requirements of paragraph 35 (1)(a). It determined it would use the personal information recorded only for the purposes of investigating suspicious or criminal activity reported, which it found to be consistent with the purpose of collection; to protect employees, detect and deter criminal activity. To limit the use of the personal information collected to that which is necessary, it determined it would restrict any viewing of the tapes to receipt of a report of crime or suspicious activity occurring in the parking lot.

After completing step four, AAA moved on to step five.

Step Five Example

After completing step four, AAA went on to step five to determine whether it has authority to disclose the personal information collected using video surveillance.

Based on the purpose of collection - to provide a safe and secure employee parking lot by detecting and deterring crime in the parking lot - AAA anticipated it may need to disclose the personal information contained in the video surveillance records to police for the purposes of investigating criminal activity in the parking lot. AAA examined section 36 and determined it could rely on paragraphs (c) and (l) for this disclosure. The authority to disclose this personal information to police was built into a guidance document prepared for its employees responsible for disclosure.

After completing step five, AAA moved on to step six.

Step Six Example

After completing step five, AAA went on to step six to determine what security and retention requirements were needed to adequately secure and retain the personal information collected by video surveillance in accordance with the ATIPP Act.

AAA previously identified the sensitivity of the personal information as moderate. However, in recognition that it may inadvertently collect more sensitive personal information, AAA decided to implement strong security controls and limited retention to adequately protect the personal information collected.

First, it identified the rules employees must follow with respect to the video surveillance of its employee parking lot:

- *The video surveillance recording equipment shall be stored in a locked room adjacent to Security Services. Only the Security Supervisor and the Head of Security shall be authorized to access the locked room and the recordings.*
- *Digital recordings shall be date and time stamped and numbered. They are to be maintained for 48 hours. After 48 hours each recording shall be deleted unless prior to the time the recording is deleted a report of criminal activity in the parking lot is received or a request for access to information under the ATIPP Act is received. If a report or an access request is received, the recording shall be placed in a secure file and retained in accordance with the retention schedule. The Security Supervisor is responsible for all aspects of managing the video recordings.*
- *Reports of criminal activity will be received by Security Services.*
- *Viewing of recordings will only occur if the Security Supervisor reasonably believes, based on a report received or otherwise, criminal activity occurred in the employee parking lot.*

- *Prior to viewing a recording, the Security Supervisor will request approval in writing from the Head of Security to view a recording or recordings and include the date or date range of the recordings to be viewed. The Head of Security will review the request and issue his or her decision.*
- *Only the Security Supervisor has authority to view the recordings.*
- *Prior to viewing a recording, the Security Supervisor shall record in the Recordings Viewing Database, his or her name and employee number, the reason for viewing the recording, the date and time the viewing occurred, the dates and times of the recordings viewed, and any subsequent uses or disclosures of the personal information.*
- *If, after a recording has been viewed, the Security Supervisor is of the view that a crime has occurred, he or she shall determine whether to report the crime to police.*
- *If a security breach occurs, the Security Supervisor and the Head of Security shall be immediately notified. The Security Supervisor shall take immediate steps to attempt to recover the information.*
- *The Head of Security shall notify senior management of the breach and the breach managed in accordance with AAA's Privacy Breach Management Policy.*

Second, it developed a policy to ensure the ATIPP Act and the rules it identified would be met.

Third, it delivered training to security services employees on the requirements of the policy. It also provided these employees with privacy training on their respective duties under the policy.

After completing step six, AAA moved on to step seven.

Step Seven Example

After completing step six, AAA went on to step seven to determine how it can accommodate requests for access under the ATIPP Act to the personal information collected using video surveillance.

To ensure it is able to accommodate requests for access to a video surveillance record, AAA consults an expert about how it can redact information from a video surveillance recording, such as images of individuals. The expert explains that the program purchased by AAA that produces the digital video has the ability to blur images, including faces, such that the image cannot be seen. Given this technology, AAA is satisfied it will be able to accommodate requests for access to information where redaction of third party personal information may be required.