Office of the
Saskatchewan Information
and Privacy Commissioner

June 21, 2020 - Advisory from the Office of the Information and Privacy Commissioner of Saskatchewan on police collecting personal information through bodycams

The Prime Minister on June 9, 2020, stated he supported the use of bodycams by police forces. He indicated bodycams were an idea "that's time has come". The Minister of Public Safety, Bill Blair stated:

> I believe that the presence of video evidence as can be made available under the right circumstances, following the appropriate policies respectful of Canadians' privacy interests that that video evidence can provide the best possible evidence to help inform exactly what transpired.

There are arguments in favor of police forces using bodycams and there are arguments against them having bodycams. The decision as to whether a police force uses bodycams is not one that an information and privacy commissioner should or can make. This decision is up to police chiefs and boards of the police commissioners. Once a decision is made to use bodycams, access and privacy issues become important. In fact, prior to the decision being taken, there are access and privacy issues that should be taken into consideration in designing the bodycams' program. The balance of this advisory deals with the questions that should be considered prior to and after the decision is made to use bodycams. This advisory outlines best practices for police forces when considering bodycams.

Can a police force use bodycams?

Webcams, bodycams, dash cams are all tools that exist in our society today. All tools can be used for good purposes or bad purposes. Police forces have the ability to inquire and use many different tools, bodycams are one such tool. The use of bodycams has been debated across our country. In fact police forces have undertaken pilot projects. Those opposed to the use of bodycams have made their position known. The cost to deploy body cams is known and is considerable. Keeping all this in mind, police forces and boards of police commissioners can decide whether they use this tool or not. Again, the balance of this advisory deals with the access and privacy issues that should be considered before and after the decision is made to utilize the tool of bodycams.

What access and privacy legislation might apply?

If a police force decides to deploy bodycams, police forces need to know what privacy legislation applies to that police force. *The Local Authority Freedom of Information and Protection of Privacy Act* (LA FOIP) applies to local authorities which include police forces in Saskatchewan. Part IV of LA FOIP deals with the collection, use, disclosure and protection of personal information.

What does The Police Act, 1990 say?

A board of police commissioners and a police chief are governed by *The Police Act, 1990* of Saskatchewan which provides:

> **31**(1) Where a municipality has established a police service pursuant to section 26, the board is responsible:
>
> (a) for the delivery of policing services within the municipality; and
>
> (b) for:
>
> (i) providing general direction, policy and priorities; and
>
> (ii) developing long-term plans;
>
> for the police service.
>
> (2) For the purposes of this Act and Part VI of *The Saskatchewan Employment Act*:
>
> (a) a board is deemed to be the employer of the personnel of the police service; and
>
> (b) the chief and any person holding the position of deputy chief of police are deemed to be agents of the employer.
>
> (3) Subject to subsection (4), a board may make directives that are not inconsistent with this Act or the regulations, setting general policy for the governing and administration of the police service.

The police chief's responsibilities are set out as follows:

> **35**(2) Subject to the general direction of the board and to this Act and the regulations, the chief is responsible for:
>
> (a) the management, administration and operation of the police service;
>
> (b) the maintenance of law and order in the municipality; and
>
> (c) the maintenance of discipline within the police service.
>
> (3) To carry out the responsibilities imposed on a chief of police by this Act and the regulations, the chief may:
>
> (a) appoint any personnel to positions designated by the board and assign their duties;
>
> (b) delegate to any member or civilian member any authority vested in the chief that, in the opinion of the chief, is required to properly manage the police service; and
>
> (c) make directives necessary to carry out the daily administration and operations of the police service.

What is the purpose of police using bodycams?

Before embarking on a bodycam program, a police force needs to focus on the purpose for the bodycam program. LA FOIP provides:

> **24** No local authority shall collect personal information unless the information is collected for a purpose that relates to an existing or proposed program or activity of the local authority.

It is important that the police force define the purpose at this early stage. The purpose should not be expanded after the fact as this would be viewed as function creep and may not be authorized. Is the purpose to accurately depict interactions between a police officer and a citizen? Is the purpose to protect the police officer? Is the purpose to gather evidence for court? Is the purpose to assist Crown Prosecutors? Is the purpose to assist defendants and defense counsel? Or is the purpose for our society to have a fairer justice system? It is not for me to define that purpose, but one can see that a police force would be well advised to define that purpose early so that all involved in the justice system know why this is being done.

One of the best ways of defining the purpose is to do a privacy impact assessment (PIA). This allows the police force to spend time discussing the purpose and determining the impact the program will have on the collection, use, protection and disclosure of personal information.

How should police forces notify citizens of the purpose of bodycams?

Police forces should be open and transparent. At the time of launching the program, tell police officers the purpose of the bodycam, when the bodycam is to be used, what the officer does with the video footage at the end of the shift, where it is to be downloaded to, who will have access to it, whether LA FOIP applies to the video footage and how long the video footage will be stored. Since this will affect police officers directly, they need to know the rules.

Similarly, citizens will want to know the same things because it will be their images which will be captured in the video footage. Further those police officers will need to know when and if during a particular interaction whether the bodycam is operating or not. Police forces will have to decide whether they have bodycams operating all the time or whether the police officer has the discretion to turn the bodycam on or off.

Citizens and police officers will particularly want to know if the police force is sharing the personal information with other third parties and why.

What personal information will the police force collect?

Capturing a person's image and voice is a collection of personal information. LA FOIP provides:

> **25**(1) A local authority shall, where reasonably practicable, collect personal information directly from the individual to whom it relates.
>
> (2) A local authority that collects personal information that is required by subsection (1) to be collected directly from an individual shall, where reasonably practicable, inform the individual of the purpose for which the information is collected.
>
> (3) Subsections (1) and (2) do not apply where compliance with them might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the information is collected.

Police forces should collect the least amount of personal information necessary to achieve the purpose. This is referred to as the data minimization principle, that is, only collect what is needed to achieve the purpose.

Purpose becomes extremely important. The data minimization principle puts pressure on a police officer (data collector) to record the least amount of video footage. This clearly implies that police officers will have to make the decisions to turn the bodycam on and off. Giving a police officer this discretion runs the risk of allegations that a police officer manipulated the footage collected. There will be pressure, to avoid this criticism, to have a bodycam running from prior to the beginning of the interaction to well after the conclusion of the interaction. It would appear, depending on purpose, that it is in the interest of police forces and citizens that the entire, beginning to end, interaction be recorded.

Police forces will have to determine whether all interactions with citizens will have to be recorded. Are there categories of interactions where bodycams **should** be turned on or **should** be turned off? It will be an important part of policy development to determine whether there are categories of interaction where bodycams should be turned on or should be turned off.

Can the police force use the personal information for any other purpose?

The police force has defined a purpose, authority to collect and has collected personal information for that purpose. LA FOIP provides:

> **27** No local authority shall use personal information under its control without the consent, given in the prescribed manner, of the individual to whom the information relates, except:
>
> (a) for the purpose for which the information was obtained or compiled, or for a use that is consistent with that purpose; or
>
> (b) for a purpose for which the information may be disclosed to the local authority pursuant to subsection 28(2).

Definition of purpose becomes extremely important. Bodycam footage can be used for the purpose for which it was collected. If video footage might be used for other purposes, then the consent of the individual or individuals in the image would have to be obtained. That can be problematic when there are multiple individuals in the video footage, some of whom are not identified.

Who can the police force share the personal information with?

Since the police force has collected the video footage (personal information), the police force needs to determine who in the organization needs to know, in other words, who will have access to the video footage. LA FOIP provides:

> **28**(1) No local authority shall disclose personal information in its possession or under its control without the consent, given in the prescribed manner, of the individual to whom the information relates except in accordance with this section or section 29.
>
> (2) Subject to any other Act or regulation, personal information in the possession or under the control of a local authority may be disclosed:
>
> (a) for the purpose for which the information was obtained or compiled by the local authority or for a use that is consistent with that purpose;
>
> (b) for the purpose of complying with:

(i) a subpoena or warrant issued or order made by a court, person or body that has the authority to compel the production of information; or

(ii) rules of court that relate to the production of information;

(c) to the Attorney General for Saskatchewan or to his or her legal counsel for use in providing legal services to the Government of Saskatchewan or a government institution;

(d) to legal counsel for a local authority for use in providing legal services to the local authority;

(e) for the purpose of enforcing any legal right that the local authority has against any individual;

…

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met;

(h) pursuant to an agreement or arrangement between the local authority and:

(i) the Government of Canada or its agencies, Crown corporations or other institutions;

(ii) the Government of Saskatchewan or a government institution;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(h.1) for any purpose related to the detection, investigation or prevention of an act or omission that might constitute a terrorist activity as defined in the *Criminal Code*, to:

(i) a government institution;

(ii) the Government of Canada or its agencies, Crown corporations or other institutions;

(iii) the government of another province or territory of Canada, or its agencies, Crown corporations or other institutions;

(iv) the government of a foreign jurisdiction or its institutions;

(v) an international organization of states or its institutions; or

(vi) another local authority;

(i) for the purpose of complying with:

(i) an Act or a regulation;

(ii) an Act of the Parliament of Canada or a regulation made pursuant to an Act of the Parliament of Canada; or

(iii) a treaty, agreement or arrangement made pursuant to an Act or an Act of the Parliament of Canada;

(j) where disclosure is by a law enforcement agency:

(i) to a law enforcement agency in Canada; or

(ii) to a law enforcement agency in a foreign country;

pursuant to an arrangement, a written agreement or treaty or to legislative authority;

(k) to any person or body for research or statistical purposes if the head:

(i) is satisfied that the purpose for which the information is to be disclosed is not contrary to the public interest and cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates; and

(ii) obtains from the person or body a written agreement not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(l) where necessary to protect the mental or physical health or safety of any individual;

(m) in compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased;

(n) for any purpose where, in the opinion of the head:

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or

(ii) disclosure would clearly benefit the individual to whom the information relates;

(o) to the Government of Canada or the Government of Saskatchewan to facilitate the auditing of shared cost programs;

(p) if the information is publicly available, including information that is prescribed as publicly available;

(q) to the commissioner;

(r) for any purpose in accordance with any Act or regulation that authorizes disclosure; or

(s) as prescribed in the regulations.

The Local Authority Freedom of Information and Protection of Privacy Regulations (LA FOIP Regulations) provides:

10 Other disclosure of personal information 10 For the purposes of clause 28(2)(s) of the Act, personal information may be disclosed:

…

(b) to an individual or body providing consulting or other services to a local authority if the individual or body agrees not to make a subsequent disclosure of the information in a form that could reasonably be expected to identify the individual to whom it relates;

(c) where disclosure may reasonably be expected to assist in the provision of services for the benefit of the individual to whom the information relates;

> (d) to a professional association or professional regulatory body for the purpose of carrying out the lawful activities of the association or body;
> …
> (f) for the purpose of commencing or conducting a proceeding or possible proceeding before a court or tribunal;
> …
> (h) with respect to health care information, in compassionate circumstances, unless the person to whom the information relates requests that the information not be disclosed;
>
> (i) to another local authority or a third party in order to obtain information from that local authority or third party to respond to an inquiry from the individual to whom the information relates, to the extent necessary to respond to that inquiry;
>
> (j) to another local authority or a government institution to enable that local authority or government institution to respond to an inquiry from the individual to whom the information relates, to the extent necessary to respond to that inquiry; or
>
> (k) by forwarding to another local authority or government institution a correspondence received from an individual to enable that government institution or local authority to reply directly to the individual where a direct reply is considered more appropriate; or
> …
>
> (n) to the investigation observer appointed pursuant to section 91.1 of The Police Act, 1990.

When we talk about sharing, we are talking about sharing with other organizations. Section 28 lists many exceptions. It does allow police forces to share video footage containing personal information with other police forces under certain circumstances. When a police force receives a request from another police force, it needs to review section 28 to see if the request involves the circumstances where sharing is permitted. LA FOIP Regulations, section 9, lists those bodies that are law enforcement agencies including the RCMP, the Chief Coroners' Office, the Special Investigations Unit of SGI, the Public Complaints Commission and the Saskatchewan Police Commission and board of commissioners under *The Police Act, 1990*.

Best practice would suggest that the bodycam policy developed by a police force indicate who, under normal circumstances, a police force might share video footage.

Best practice would suggest that a police force apply the data minimization rule. This rule says, provide the least amount of information (video footage) required to meet the request. Further, best practice would suggest that video images of persons other than those that are the subject matter of the request should be blurred or de-identified.

Is the police force obliged to protect the video footage?

The video footage with personal information the police force has collected must be protected. Once the police officer takes video footage with personal information, it is the police force's obligation to ensure it is protected. LA FOIP provides:

> **23.1** Subject to the regulations, a local authority shall establish policies and procedures to maintain administrative, technical and physical safeguards that:

(a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control; or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

Because we are talking about video and audio images, we are talking about electronic storage. This means storing the information on servers. A police force needs to make a decision as to whether servers are located in police force offices at an IT service provider in the province or Canada. This is generally referred to as the Cloud. Best practice would dictate a police service select the option that would give it the greatest amount of security and protection.

When should the police force destroy the video footage (personal information)?

How long is a police force going to keep bodycam footage which obviously contains personal information? Will it get destroyed in accordance with the destruction of records policy? Should it have a special destruction period, shorter or longer than the normal? Will the video footage be evidence in a Court case? Police forces will need to develop a policy which will specifically include destruction of video footage.

Do police forces need to be transparent about bodycams?

As with any tool used by an organization, it can have good effects and bad effects. The risk of bad effects creates fears of the misuse. Best practice would suggest to build trust and confidence. A police force should be transparent in its position on bodycams, their use and security of the information. The best way to do this is to provide information on its website about its bodycam program. Transparency would start with developing a policy on bodycams as discussed below.

Do police forces need to create a policy regarding bodycams?

Once a police force has made a decision, the police force should consider some documentation of the plan. Prior to a police force making its decision on bodycams, best practice would suggest they do a privacy impact assessment. This exercise will surface the privacy issues that a police force will encounter in designing the program, implementing the program, developing policies and communicating with the public.

One of the essential steps would be to develop and make public a policy on its bodycam program. The policy should contain:

- a statement of the authority;
- a statement of the purpose;

- a statement on possible actions taken with video footage, its collection, storage, protection and use;
- a statement on how and where video footage will be stored;
- a statement as to who within the police force will have access to the video footage;
- a statement that the video footage containing personal information will be shared will only those within the police force that need-to-know and will not be available within the police force;
- a statement on how the video footage containing personal information will be protected;
- a statement as to how and when it will be shared with other police forces and law enforcement agencies; and
- a statement as to when the video footage containing personal information will be destroyed.

A policy should be made available to staff, and citizens and posted on the police forces' website.

Can I request videos taken of me?

> **30**(1) Subject to Part III and subsections (2) and (3), an individual whose personal information is contained in a record in the possession or under the control of a local authority has a right to, and:
>
> (a) on an application made in accordance with Part II; and
>
> (b) on giving sufficient proof of his or her identity;
>
> shall be given access to the record.

A citizen does have the right to request access to video footage concerning that citizen. There are exceptions to this rule and those exceptions can be found in Part III (sections 13-22) of LA FOIP. A citizen does not have the right to view images of other citizens that may be in the video footage. A video can easily capture multiple individuals and a citizen does not have the right to the images of other individuals. When an access request is made, a police force would have to carefully review the video footage, blur out the images and delete the audio track of others.

Conclusion

The principles are simple; establish the purpose, authority, and collect the least amount of personal information to meet the purpose, share it only with those who need-to-know, store it, keep it secure and destroy it when no longer needed. This is good advice for police forces or any other organization.

References

For more information on police and bodycams see:

- Video Surveillance Guidelines for Public Bodies (January 2018);
- Guidance for the use of body-worn cameras by law enforcement authorities

Media contact:
Kim Mignon-Stark
Kmignon-stark@oipc.sk.ca