Calgary Police Service

Body Worn Cameras (BWC) and In Car Digital Video (ICDV) Privacy Impact Assessment

2015
September 16

Privacy Impact Assessment:

Body Worn Cameras (BWC) and In Car Digital Video (ICDV)

Calgary Police Service

EXECUTIVE SUMMARY

The Calgary Police Service (CPS) is adopting body worn camera (BWC) technology, the purpose of which is to support CPS officers in the execution of their common law and statutory law enforcement and policing duties. The utilization of the BWCs will occur within a framework aimed to balance those needs against the privacy rights of individuals. At the same time, officers will be using police vehicles equipped with In-Car Digital Video (ICDV).

Although BWC is a relatively new tool for law enforcement, the CPS has benefited from the experience with BWCs in communities in the United Kingdom and the United States. This includes research undertaken by the UK Home Office and by the USA Department of Justice. The CPS hosted an international workshop in 2014 to learn more about the experience in other jurisdictions with BWCs. The CPS has also collaborated with the police services in Edmonton and Toronto in investigating BWCs and is grateful for their assistance.

The use of this technology can be privacy-invasive. The CPS is a local public body for purposes of the *Freedom of Information and Protection of Privacy Act* ("*FOIP*") and is required to comply with the requirements of that Act. Compliance with *FOIP* is overseen by the Alberta Information and Privacy Commissioner. The CPS has voluntarily undertaken this Privacy Impact Assessment to ensure that it has identified the privacy issues and risks associated with BWCs and that it has appropriate measures to mitigate these risks.

The kinds of risks associated with BWCs that have been identified by the Alberta Information and Privacy Commissioner and her colleagues across Canada are captured by the following questions:

- Are BWC and ICDV necessary, effective, proportional to the problem and the least privacy-invasive means to address the problem?
- Will there be appropriate notification to the public of BWC generally?
- Will there be appropriate notification to individuals who will be recorded by the BWCs?
- Will the BWC recording be constant or only for specific police-citizen interactions?
- Will there be appropriate measures to avoid recording bystanders?

- Will there be proper safeguards in terms of collection, use and disclosure of personal information?
- Will there be proper safeguards in terms of retention, storage and destruction of BWC recordings?
- What, if any, use will be made of video analytics by CPS?
- Will individuals recorded by BWC have appropriate access to such records?
- Will the CPS have the appropriate policies and procedures that identify the program objectives and set out the rules governing the program?

This PIA documents the CPS's approach to the issues associated with BWC and ICDV use.

Section C of the PIA considers the collection, use and disclosure of personal information by the BWC and the ICDV, the relevant legal requirements and how each of those requirements will be met by the BWC and the ICDV. The same section also reviews the advice received from the Alberta Information and Privacy Commissioner, the Privacy Commissioner of Canada and other privacy oversight bodies in addressing the issues of necessity, proportionality, effectiveness and minimal intrusiveness.

Public notice of BWC use will be provided to the citizens of Calgary through an awareness campaign when full deployment of both technologies occurs. In addition, individuals who would be captured by audio and video of the BWC will be notified when it is safe and practicable to do so.

The BWC will not be activated throughout an officer's entire shift. It is to be activated only when there is a law enforcement related encounter and activity. Generally, the BWC will be deactivated when a specific incident, call for service or related charges are completed or when a call for service is deemed not to be a police matter. Additionally, the BWC can be deactivated so as not to record privileged conversations or in other instances where it is reasonable not to record.

Officers are directed by CPS policies including the *Body Worn Camera Policy* and will be trained to avoid recording individuals who are mere bystanders and are not victims, witnesses or suspected offenders.

Section D of the PIA considers the major privacy risks and how each will be mitigated.

Safeguards for the retention, storage and destruction of BWC recordings are addressed in both Sections C and D of the PIA. The safeguards include administrative measures, physical measures and technical measures to safeguard the personal information collected, used or disclosed through the BWC or ICDV technology. In the event of a privacy breach, the CPS has

a *Privacy Breach Guidelines* policy consistent with recommendations from the Alberta Information and Privacy Commissioner.

Those individuals who may be recorded by BWC or ICDV will have appropriate access to their personal information as required by *FOIP.* Individuals can make a request for access to records with such information and these will be processed by the CPS *FOIP* unit.

An important feature of the CPS implementation and use of BWC and ICDV is the body of relevant policies which include the following:

Body Worn Cameras

FOIP Policy

Privacy Breach Standard Operating Procedure

Information Technology

Investigative Digital assets

Records and Information Management

Property Handling

A copy of the BWC policy in included with this PIA.

In addition to the requirement to comply with *FOIP* and Orders of the Information and Privacy Commissioner, the CPS is also required to comply with other federal and provincial statutes, including but not limited to the *Youth Justice Act*, R.S.A. 2000, c. Y-1, the *Child Youth and Family Enhancement Act*, R.S.A. 2000, c. C-12, the *Children First* Act, S.A. 2013, c. C-12.5, the *Police Act*, R.S.A. 2000, c. P-17 and the Federal *Youth Criminal Justice Act*, S.C. 2002, c.1, *Criminal Code of Canada*, R.S.C. 1985, c. C-46 and the Canadian *Charter of Rights and Freedoms* as well as the direction of the Alberta Minister of Justice and Solicitor General as published in the *Alberta Provincial Policing Standards Manual*. The combined effect of the legislative requirements that the CPS is subject to is further protection of personal information collected, used or disclosed by the CPS. Pursuant to the *Police Act* and the *Police Service Regulation*, oversight is provided by the Calgary Police Commission and the Law Enforcement Review Board also provides an independent and impartial review of decisions of the Chief of Police relating to complaints about the conduct of a police officer.

SECTION A - PROJECT OVERVIEW

The Calgary Police Service (CPS) will equip all frontline, uniformed personnel with BWCs. Additionally, all CPS marked vehicles equipped with lights and sirens will have ICDV installed.

The purpose of BWCs and ICDV is to support CPS officers in the execution of their common law and statutory law enforcement and policing duties. The utilization of the BWCs will occur within a framework aimed to balance those needs against the privacy rights of individuals.

CPS officers will be equipped with BWCs which will be activated in specified circumstances in the course of their duties to provide an audio and video record of their interaction with individuals. BWCs are intended to capture specific incidents. They are not intended for 24 hour recording. When a BWC is utilized, recordings will be treated as supporting the officer's observations and shall supplement, not replace, detailed notes.

The purposes of BWC use include:

- Providing additional evidence for prosecutions
- Augmenting current note taking practices and improve evidence documentation
- Increasing public trust and confidence
- Increasing police accountability
- Reducing incidences of the use of force by and against the police by affecting the behaviour of individuals who are aware of the recording in-progress
- Increasing transparency
- Reducing frivolous complaints of alleged police misconduct
- Increasing the efficiency of resolution of complaints against police
- Providing early-case resolution in prosecutions
- Providing real-life training examples.

The BWCs will be issued to officers at the beginning of their shift and then returned to a designated docking station at the end of the shift. The opportunity to view the recordings will be tightly controlled based on the role of the person seeking to view the recordings and the purpose for which the recordings are to be viewed.

A.1 RATIONALE FOR BWC & ICDV TECHNOLOGY

Police agencies in North America began using ICDV in 1980 as a means to record the driving behaviour and actions of impaired drivers. ICDV has proven to be a valuable tool to corroborate and supplement the testimony provided by police, the result of which has been successful prosecutions. With technological advancements and increased public demands

for accountability, many police agencies have implemented the use of BWCs. The CPS began investigating BWCs in 2012 and undertook a successful pilot project between 2012 November 8 and 2013 May 10.

In recent years, there has been a significant body of research and experience with BWCs that informs the approach taken by the CPS. This research includes work done by the U.S. Dept. of Justice and the U.K. Home Office to evaluate the experience with BWC technology in communities in both of those nations. The British experience as explained in a BWC symposium is that BWC have:

- Increased the number of domestic conflict convictions
- Increased appropriate custodial sentences
- Increased public confidence
- Decreased the number of citizen complaints.

In Canada, the Chair of the Civilian Review and Complaints Commission for the RCMP stated at page 67 in his December 8, 2009 Report Following a Public Interest Investigation in to a Chair-Initiated Complaint Respecting the Death in RCMP Custody of Mr. Robert Dziekanski:

> In the circumstances of this case, there would have been a clear benefit to video footage capturing the events from the members' perspectives. Although the Commission had the benefit of a non-police generated video, there is no doubt that a system that would allow all "to see and hear the event unfold through the eyes and ears of the officer at the scene,"[1] would be the best of all possible options…I believe that the time has arrived to give these devices additional consideration within the Canadian policing context.

In July 2014, the Honourable Frank Iacobucci completed an independent review for the Toronto Police Service titled "Police Encounters with People in Crisis." Following an extensive report, the Honourable Frank Iacobucci recommended, among other things, that the Toronto Police Service "issue body worn cameras to all officers who may encounter people in crisis to ensure greater accountability and transparency for all concerned".[2]

Canadian courts have also considered the usefulness of evidence in the form of police generated video. In *R. v. Hughes*, 2014 ONCJ 105 (CanLii), the Court considered evidence from an ICDV and came to the conclusion, at para. 44 of the decision, that: "Simply put, the

[1] *Guidance for the Police Use of Body-Worn Video Devices*, Home Office (Police and Crime Standards Directorate), July 2007, at p. 5.

[2] *Police Encounters with People in Crisis, An Independent Review Conducted by the Honourable Frank Iacobucci for Chief of Police William Blair, Toronto Police Service*, July 2014, at p. 263

in-car camera video is the best evidence of the offense, essential not only to possible *Charter* motions but also the applicant's ability to make full answer and defence."

The CPS was also able to gather much useful information from a 2014 International BWC Symposium it hosted. That included information that BWCs have significant potential to enhance public safety, contribute to officer training, reduce public complaints, prevent negative interaction between police and members of the public and significantly increase public trust and confidence.

A.2 DESCRIPTION OF THE BWC SYSTEM

At the start of a shift, the operator trained on the BWC system will ensure the BWC equipment is operating properly and is placed on the uniform. A notation of the use of a BWC will be entered in his or her notebook.

The BWC will be activated and de-activated during the course of a shift. BWC recording will be initiated at the commencement of an interaction between the CPS member and a member of the public in accordance with the applicable BWC policy. When practicable and safe to do so, members of the public will be advised that they are being recorded. In the event the BWC is deactivated, the members must make a notation in their notebook as to the reason for the deactivation as well as, when possible, record a statement on the device with the reason for deactivation.

At the end of the shift the BWC will be placed in the designated charging system to upload all recordings and to charge the BWC. The BWC recordings will be uploaded automatically from the docking station to a secure, centralized server maintained by the Information, Communication and Technology Section. BWC recordings will be erased after 13 months unless required as evidence. In that case it will be retained according to the CPS Records Retention Schedule.

BWC and ICDV video is recorded in order to create a record of police interactions with the public that are directly related to their law enforcement and policing duties. This may include traffic stops, responding to calls for service, conducting investigations, and detaining or arresting an individual. Collection of personal information in these circumstances is consistent with and permissible according to s. 33(b) of *FOIP*. During recording, a variety of personal information may be collected. Due to the nature of how this tool is intended to be used, the personal information collected at any given time will vary. However, all videos recorded will be subject to rigorous access management protocols.

Access to BWC recordings is strictly controlled and is permitted only in accordance with the CPS BWC policy. Access is permitted for investigative reasons, including internal investigations and for law enforcement purposes. Viewing by an officer who was present at

the scene but who did not record the video in question may only occur with the permission of the officer whose BWC actually captured the video and the officer who did not record the video may only view the recording for the time period during which he or she was present at the scene or for law enforcement or policing purposes.

Additionally, the recording devices prevent end-users from modifying or deleting any videos at source. Control over the videos is limited to the BWC Coordinator. Videos will be downloaded from the recording device directly to the CPS network. This is an automated process, controlled via the vendor's proprietary back-end software. The proprietary nature of the vendor's software also makes it impossible to view the videos on any system other than the authorized CPS system.

Finally, the officer's regimental number (employee ID), time and date of recording, and other metadata are automatically associated with the video. The back-end software specifically controls access to each file, only allowing the individual who recorded it and the BWC or ICDV Coordinator to access the video (or set permissions for additional viewers). All access is tracked and the software maintains a chain-of-custody audit report. The secure BWC software ensures and maintains the integrity of video continuity. The continuity log will track each time a video is accessed. BWCs feature internal storage that is not removable, nor is it accessible by the assigned police officer.

The secure BWC software downloads the video from the BWC and logs all activity from the time the file is recorded to the time it is downloaded into the secure software program. This creates an entry on a continuity log that is traceable to the individual CPS officer, BWC, and BWC video. Any time a BWC video is reviewed, tagged, or transferred in any manner, an entry is generated in the continuity log. A continuity log for all BWC video is generated and maintained automatically by the BWC itself and the secure BWC software.

Should BWC or ICDV video be of evidentiary value in cases where charges are laid in relation to a recorded incident or where the BWC recording forms part of the evidentiary record in cases where prosecutions are initiated, the video will be disclosed to the Crown in accordance with the applicable laws relating to disclosure . Upon disclosure to the Crown, use and further disclosure of the video is under the authority of Crown counsel according to the rules of criminal procedure. In many cases it is expected that the Crown will disclose the video evidence to defence counsel and, ultimately tender the video as evidence in court. Videos that remain in the possession of the CPS will be subject to the investigative retention schedule.

A more detailed consideration of the parameters with respect to BWC activation and deactivation as well as some special considerations related to whether the BWC or ICDV should be utilized are as follows:

BWC Activation Parameters

1. Upon activation and whenever safe and practicable to do so, members will verbally state the date, time, location, and nature of the incident.

2. If an officer's vehicle is equipped with ICDV, members will also utilize that system in accordance with ICDV policies and procedures. Members will then activate the BWC when arriving at a call to ensure continuity of the entire event. In some circumstances, it may be necessary to have both systems simultaneously recording.

3. When more than a single officer equipped with a camera is at the scene, each member will activate their respective BWC in keeping with policy.

4. Where it is safe and practicable to do so, members will use the BWC or ICDV to record investigative contact which is defined in the BWC policy as any direct contact between a police officer and a member of the public where that contact is for the purpose of a police investigation. Investigative contact may include, but is not limited to:

    a) Calls for service;

    b) Investigative detention;

    c) Apprehensions under the *Mental Health Act*, R.S.A. 2000, c. M-13;

    d) Arrests;

    e) Interactions with persons in crisis

    f) Crimes in progress;

    g) Investigations.

In addition to the investigative contact described above, BWC or ICDV may, where it is safe and practicable to do so, be used in circumstances including, without limitation,

1. Primary disclosure from a witness or victim of a crime who is providing their first account of the incident with due consideration to the sensitivity and nature of the offence being investigated, and any potential threat to the safety of the individual that may arise through disclosure;
2. The obtaining of a waiver to provide a statement from a youth;
3. Foot pursuits;
4. The execution of a consent search or a search warrant;

5. Calls where individuals are either mentally distressed, impaired by drugs or alcohol or otherwise behaving in a manner which may be considered altered or irrational;
6. Any encounter with the public that may become adversarial after the initial contact;
7. Documentation of an accident or crime scene, in accordance with the provisions of this section;
8. The collection of evidence that may be used in the prosecution of an offense;
9. Anytime a dynamic or forced entry is made into a residence; and
10. Domestic dispute related calls.

BWC Deactivation Parameters

1. As a general guideline, the BWC or ICDV will be deactivated in the following circumstances:

   a) A specific incident, call for service, or related charges are completed and the purpose for activation is no longer present;

   b) A call for service, or any other incident, is deemed not to be a police matter;

   c) Engaging in conversations containing privileged information (receiving legal advice from a Crown Prosecutor, speaking to a known confidential informant, etc.);

   d) When attending a lawyer's office, unless responding to a call for service;

   e) Any other instance where it is reasonable and justifiable.

2. Prior to deactivation, members shall, when safe and practical to do so, state the time, place and reason for deactivation and/or record it in the member's notebook.

3. If the BWC or ICDV is reactivated during the same incident, the reason for reactivation should be verbalized and documented in the member's notebook and in any related record management system ("RMS") report.

4. Accidental deactivation of the BWC or ICDV shall be documented in the member's notebook and any related PIMS occurrence (RMS) report.

Special Considerations for Recording or Not Recording

1. Citizen objection to recording

Members may encounter situations where one party objects to the recording taking place. Generally it is recommended that members continue to record notwithstanding the objection as consent is not required when the recording occurs in the context of law enforcement and policing activities. The member may provide reasons to the individual for continuing to record when an objection has been made. For example, the member may advise:

i. that an incident has occurred requiring police to attend;

ii. that the member's continued presence might be required to prevent a breach of the peace or injury to any person;

iii. the member's duty is to secure the best evidence available, with emphasis given to the accurate depiction of the incident in the interest of all parties present;

iv. that continuing to record would provide an additional record of any significant statement made by any party;

v. that continuing to record will safeguard the complainant and the member from any potential allegations from any party.

2. Private Dwellings

If a member attends a private dwelling for an incident that would normally be recorded in the member's notebook, the BWC should be activated. Members should be mindful of the citizen's expectations of privacy and, if possible, avoid recording any person or anything inside the dwelling that is unrelated to the original incident.

3. Domestic Violence

Reports of domestic violence are a priority for the CPS. BWC or ICDV can capture detailed evidence in these situations. Every effort should be made to activate and keep the BWC or ICDV recording, with any objections handled in accordance with professional responses outlined in the applicable policies.

Scene examination photographs and capturing of injuries sustained should be referred to the Forensic Crime Scenes Unit for attendance, as outlined in the Investigative Digital Assets Policy.

4. Sexual Assault

While BWC or ICDV recordings may be a potential benefit in capturing important evidence, sensitivity must be employed by members responding to sexual assault complaints. If the complainant is a child or youth, child abuse protocols must be followed.

5. Young Persons

BWC or ICDV is to be used accordingly when young persons are provided access to their parents and/or legal counsel.

6. Witness and Victim Statements

A member wearing a BWC or ICDV microphone may interact with victims or witnesses who are giving their first account of an incident. Any initial disclosure from such persons will be treated as an evidentiary recording. While capturing verbatim accounts from victims and witnesses has inherent benefits, members should be mindful of the sensitivity of the information being reported, coupled with any potential threat to the safety of the individual that may arise as a result of disclosure.

BWC or ICDV recordings do not replace the need for formal written statements from victims or witnesses and the use of video recorded interview rooms. KGB statements will be administered within the realm of a CPS facility in accordance with Calgary Police Service Policy on administering KGB statements.

7. Places of worship and religious institutions

If a member attends a place of worship for an incident that would normally be recorded in the member's notebook, the BWC should be activated. Members should be mindful of the sensitive nature of recording within a religious institution and, if possible, avoid recording any person or anything inside the place of worship that is unrelated to the original incident.

Recording Restrictions

Generally speaking, CPS Members will not record:

i. Their entire shift;

ii. Their own administrative duties or the activities of other members that are not complaint or charge related;

iii. Activities in the Administrative (non-custodial) areas at the Court Services Section;

iv. A static point assigned at a major event unless circumstances arise;

v. In a law or medical office, except when responding to an emergency call for service originating from (inside) the law or medical office;

vi. Investigative discussions or inquiries between officers;

vii. During a situation that would reveal police investigative or tactical techniques;

viii. In a covert manner;

ix. Interactions with a Confidential Informant; and,

x. Places where a reasonable expectation of privacy exists (e.g. bathrooms or locker rooms) except when responding to an emergency call for service or an in view situation in respect of such a location.

Prohibitions

Officers are prohibited from the following:

i. Recording video playback of another BWC or ICDV device;

ii. The access or dissemination of BWC or ICDV video to any person or outside entity, unless pursuant to disclosure obligations or lawful police purposes;

iii. Using BWC or ICDV for the purpose of covert recordings of incidents.

A.3 KEY STAKEHOLDERS

The ICDV and BWC project and the use of BWC and ICDV impact the Service in many ways both internally and externally. A list of identified stakeholders includes:

- Member of the public who has contact with an officer wearing a BWC or using an ICDV
- The officer wearing the BWC or using the ICDV
- Supervisors who review charge disclosure packages
- Disclosure technicians preparing disclosure packages for presentation to the Crown
- Crown Prosecutors and their staff who review the disclosure packages for completeness
- Defense counsel and/or accused persons who obtain the disclosure materials from the Crown
- The Court in the review of evidential images and recordings
- Information Technology Security management who conducts audits on the use and dissemination of data within the Service
- Personnel within the Service *FOIP* Section who are responsible for facilitating access to records and protecting personal information.

SECTION B - ORGANIZATIONAL PRIVACY MANAGEMENT

B.1 MANAGEMENT STRUCTURE

The Chief of Police is the head of the CPS, by definition under *FOIP*.

By virtue of a delegation instrument, revised 2005 January 19, the Chief of Police has delegated responsibility for ensuring the protection of personal information under s. 38 of *FOIP* to all Section Managers and Commanders within the CPS.

The CPS Privacy Counsel/*FOIP* Manager acts as the privacy and access subject matter expert for the CPS. The Privacy Counsel/*FOIP* Manager acts in a consultative role in all CPS projects involving the potential collection, use and disclosure of personal information, provides legal opinions to all members of the CPS in respect of privacy and access matters, and provides advice and direction in the development of privacy-compliant practices and processes.

Under the management of Privacy Counsel, the *FOIP* Section of the CPS has a mandate that includes advising all areas of the Service with the privacy provisions of *FOIP* to ensure compliance. Other duties undertaken by the *FOIP* Section include:

- Administering the *FOIP Act* for the CPS.
- Managing and facilitating requests for information under *FOIP* pursuant to the authority delegated by the Chief of Police.
- Advising on the release and withholding of personal information under *FOIP*.
- Providing counsel on legal and policy issues arising from *FOIP*.
- Representing the CPS in dealings with the Office of the Information and Privacy Commissioner and on judicial review.

All CPS members are obliged to comply with the privacy protections afforded by *FOIP* and policy, as well as the requirements of the *Police Act*, *Police Service Regulation*, *Criminal Code* and *Youth Criminal Justice Act* and to remain current with all policies and procedures of the Service, including new Directives.

B.2 POLICY MANAGEMENT

Relevant policies include:

Body Worn Cameras

FOIP Act Policy

Privacy Breach Standard Operating Procedure

Information Technology

Investigative Digital assets

Records and Information Management

Property Handling

The policy specific to BWC and ICDV usage is attached in Part E of this document. These policies within the CPS have been developed in consultation with the *FOIP* Manager of the CPS. In general, CPS policies provide detailed and comprehensive guidelines (applicable to both sworn and civilian members) regarding the collection, access, use, disclosure, retention, and destruction of personal information. More specifically, CPS *FOIP* policy, s. 7 mandates that access to information contained in any database is permitted only for legitimate law enforcement duties. This same policy requires that section 38 *FOIP* requirements are met with respect to protecting personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction of records; ensuring privacy is maintained; and following the Records Retention Schedule.

All CPS policies are reviewed by a Review of Policy and Procedures Committee and upon approval by the Committee, they are then approved by all Senior Executive Members before receiving final sign off and promulgation as Directives to all members of the Service.

The BWC and ICDV project team has consulted with the *FOIP* Section and other legal advisors within the Service. One item of note is the current lack of any specific Canadian case law related to the collection, use and management of video recorded files from BWC devices. The CPS will monitor the developing jurisprudence in relation to the use of BWCs and will review its policies in light of emerging legal principles to ensure continued compliance with legal requirements. All CPS members are obliged to remain current with all policies and procedures of the Service, including new Directives.

B.3 TRAINING AND AWARENESS

An effective training and awareness program is an essential aspect of the CPS risk mitigation strategy. In addition to standard CPS privacy training on *FOIP* and data security, officers being issued BWCs will be trained on the following as part of the implementation of this initiative:

- Proper operation of the BWC or ICDV device
- Specific locations where the cameras or recording may be turned off due to an increased expectation of privacy
- How to address concerns of individuals being recorded and issues around the topic of "consent"

- CPS policy on the creation, storage, disclosure and retention of video from BWC and ICDV devices.

The CPS security guidelines, BWC and ICDV policy and BWC and ICDV SOPs are available electronically for camera users to review at any time.

Compliance with training requirements is monitored by supervisors within the various work areas throughout the Service.

B.4 WORK FLOW ANALYSIS

In general, CPS members are responsible and accountable for the collection of police information. The CPS is involved in crime prevention, maintaining the peace, protecting people and communities, intelligence work and enforcing the law. Duties of police officers include: apprehending criminals, other offenders and others who may lawfully be taken into custody, laying charges and participating in prosecutions, executing warrants that are to be served by police officers, assisting victims of crime and performing other related duties.

Law enforcement requires the collection of personal information. Law enforcement agencies, including police services, are authorized by *FOIP* to collect personal information for law enforcement purposes and otherwise as authorized by law.

Alberta's police services, with the exception of the RCMP, are governed by *FOIP*. This Act establishes the legislative framework within which police services collect personal information. Each police service is responsible for ensuring that its policies and procedures as well as the actions of its members comply with the privacy provisions of the Act. Police services must also comply with the privacy provisions in other legislation such as the federal *Youth Criminal Justice Act*.

The CPS will continue to be governed by *FOIP* and various other pieces of legislation with respect to its collection of personal information. As a public body, the CPS is responsible and accountable for its compliance with *FOIP*.

B.5 INFORMATION FLOW ANALYSIS

Videos will be recorded on the BWC or ICDV device. The storage media is securely stored within the device, and cannot be directly accessed by the user. At the end of a shift, the police officer assigned to that BWC device will place it on a docking station and an automated process will download the video to the CPS storage network. In the case of ICDV, the recordings are stored in a storage device in the patrol vehicle. When the vehicle returns to the District Office, the information is uploaded by a secure wireless connection to the CPS storage server.

A Role Based Access Control will be in place as per the vendor supplied software. Additionally, auditing tools within the CPS Information Technology network are used to create logs which can be utilized by security professionals and management to investigate or detect unauthorized use and access to private information. Retention rules have been developed to align with similar requirements such as s. 35 (b) of *FOIP* and the *Alberta Provincial Policing Standard Manual* Section 6.4.

If a recording contains evidentiary information, it will be bookmarked and tagged so that it is properly associated to the investigative file and managed as digital evidence under the CPS Investigative Digital Asset policy. If charges are laid, the video may be disclosed to the Crown. CPS has a centralized Court Disclosure Unit and only specially trained individuals will have access to the video for the purpose of creating a Disclosure package for the Crown (*FOIP* s. 40(1)(c)). Information consistent with what would normally be vetted from officer written notes will be redacted from the video in accordance with section 40(4) of *FOIP*.

If a recording contains no evidentiary information, it will be retained and stored electronically as a record of the service in accordance with the CPS Investigative Digital Asset policy, and will be retained for a period of thirteen months in accordance with the Director of Law Enforcement policy on Policing Standards. These recordings will be accessible only in accordance with *FOIP*. The recordings can be viewed internally for authorized law enforcement and policing purposes only. The retention of these recordings will be managed through the CPS Records and Information Management policy.

Sample Information Flow

- Video captured by officer in the field.
- BWC Device docked/ICDV Video transferred to network.
- Video tagged and bookmarked.
- Video access permissions recorded as part of permanent record associated with the video.
- If part of a charge package: Court Disclosure Unit prepares copy for Crown (redaction occurs).
- Retention rules applied.

B.6 INCIDENT RESPONSE

In the event that there are any violations of the policies and procedures that lead to an unplanned or unauthorized disclosure of personal information captured on BWC or ICDV, the CPS has in place a comprehensive policy to respond to and manage the issue. CPS Privacy

Breach Guidelines are modeled on the OIPC publication *Key Steps in Responding to Privacy Breaches*. The four guiding principles are designed to ensure:

- Containment of any breach;
- A proper evaluation of any risks associated with the breach;
- That notification occurs where appropriate; and
- That future breaches are prevented.

The CPS ICTS has an entrenched Incident Response Plan which will be utilized upon identification of any unauthorized access or ICTS security concern or issue. The complete Incident Response Plan is attached in the Appendix to this PIA.

SECTION C - PRIVACY ANALYSIS

C.1 LEGAL AUTHORITY

Freedom of Information and Protection of Privacy Act

FOIP applies to all records in the custody or under the control of a public body. "Public body" is a defined term in *FOIP* and includes a local public body [s. 1(j)]. A local public body is defined in s.1(p)to include a "local government body". A "local government body" includes a "police service"[s. 1(i)(x)(B)]. The Calgary Police Service therefore qualifies as a public body for purposes of *FOIP* and is therefore subject to *FOIP*.

Part I of *FOIP* provides that individuals can make an access request to a public body and sets out the procedures to do that. Part II is concerned with the protection of privacy. It sets out the rules by which a public body can collect, use or disclose personal information of individuals. The right of access to records held by a public body is balanced by the need to protect an individual's personal information. The collection, use and disclosure of personal information may be reviewed by the OIPC upon the request of an individual in order to ensure that the public body's decisions with respect to the disclosure of records are in compliance with the Act. *FOIP* also provides a means for the public to make a complaint to the OIPC if they believe their information has been collected, used or disclosed in violation of the Act.

FOIP is a type of law characterized by the Supreme Court of Canada as 'quasi-constitutional'. It is paramount to other provincial laws in the event of a conflict between another provincial law and *FOIP* unless the other law is declared in legislation or regulation to be paramount.

Federal and Provincial Privacy Commissioner Orders and Guidelines

In addition to addressing the legislative and regulatory requirements that will apply to BWC and ICDV, already described above, this PIA also considers orders, recommendations and best practices identified by the Alberta Information and Privacy Commissioner as well as other privacy oversight offices in Canada. Not surprisingly, given the novelty of the police use of body worn cameras in Canada, the CPS has found that there is a paucity of material from those offices directly on point.

Although the OIPC has not directly addressed the question of police BWCs or ICDV in any of its formal orders or reports, there are a number of Orders that address records, including personal information of individuals, held by Alberta police services. In many of these orders, the focus is on what happens to personal information subsequent to collection. In other words the issue is one of improper use or disclosure of personal information in the custody of a police service. These reports are helpful in understanding what may be required for purposes of complying with *FOIP*.

In Orders 96-019 and 2001-027 the Alberta OIPC interpreted the meaning of the term "law enforcement record." Orders 2000-027 and F2015-26 also provide clear guidance on the meaning of "policing" as it relates to the Act.

OIPC Order F2006-033 dealt with interpretation of s. 38 as well as ss. 33 (collection) and 39 (use) of *FOIP*. OIPC Orders F2006-033 and F2006-029 are important since they adopt an approach developed by courts for the Crown's evidentiary obligations when discussing a police officer's standard practice.

The OIPC also considered "collection" and "use" of personal information by a police service in terms of an electronic database in several orders. These include Orders F2006-029, F2007-030 and F2008-024.

Although not dealing with collection, use or disclosure or security of personal information, the Alberta OIPC Order F2009-013 highlighted the exclusion from *FOIP* for ongoing prosecution records. The exclusion is found in s. 4 (k) of *FOIP* and is for "a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed." At some point, some of the BWC material and personal information of individuals will be transmitted to the Crown Counsel for prosecution. The focus of this PIA, however, is on the law enforcement activities and work of the CPS.

In addition to the guidance provided by Alberta OIPC Orders the Federal Privacy Commissioner is also a source of information relevant to the implementation of BWC and ICDV. In 2011, the Privacy Commissioner of Canada, who oversees the RCMP and its compliance with the *Privacy Act*, R.S.C. 1985, c. P-21, issued an audit report entitled *Audit of Selected RCMP Operational Databases*. This focused on CPIC and PROS. CPIC is the

Canadian Police Information Centre and provides computerized storage and retrieval of information on crimes and criminals. PROS is the Police Reporting and Occurrence System and is the RCMP's primary operational records management system. The audit stated in part:

> Both CPIC and PROS contain extensive sensitive personal information that, if improperly used or disclosed, could have a significant impact on the rights and freedoms of individuals as well their reputations, employability and safety. A security breach may also compromise ongoing police investigations. The RCMP reports annually on security breaches related to the CPIC system. Many of these breaches have involved unauthorized access to and inappropriate use of personal information, with potentially significant privacy implications for the individual whose information was accessed." [p. 3]

In discussing CPIC, the report observes at p. 4 that: "Many of the breaches involved users querying CPIC for personal reasons." In another part of the same report, at p. 5, it is stated that: "There is no active review of PROS user accounts. While the RCMP's PROS policy requires that a user's access be revoked when no longer required to perform job functions or after 14 months of inactivity, we found there were over 1,000 users with active accounts who had not accessed PROS for a period of 14 months or longer. We also found the process used to review user activity on PROS to be cumbersome, rendering reported incidents of misuse difficult to investigate."

The RCMP audit by the PCC also revealed one of the reasons why it was difficult to investigate reported misuse of the system (PROS) was that an automated audit log review tool had not been implemented and without it, extracting details of a user's activity is highly labour intensive.

In addition to formal Orders, the Alberta OIPC website also offers a number of resources to assist in interpreting and applying *FOIP*. These include:

- Literature Review on Issues of Privacy and Surveillance Affecting Social Behaviour
- Privacy Breach Guidelines
- Guidelines for Overt Surveillance in the Private Sector.

One section of the OIPC website involves summaries prepared by bodies subject to OIPC oversight that outline PIAs they have submitted to the OIPC for review and acceptance by the OIPC but not approval. Submitting PIAs is a requirement for custodians under the *Health Information* Act, R.S.A. 2000, c. H-5 ("HIA") who are contemplating new information systems/technology. It is a recommended practice for public bodies subject to *FOIP*. Below

are descriptions of several relevant PIAs that have been accepted by the OIPC and reviewed by the CPS in conjunction with the preparation of this PIA:

a) Public Body or Custodian: Edmonton Police Service Project Title: Body Worn Video Pilot Date Submitted: February 3, 2012 Date Accepted: May 18, 2012 OIPC TRAX File:

> F6114 Project Summary: The Edmonton Police Service is undertaking a pilot project from October 2011 to September 2014 to research the efficacy of a new law enforcement tool, body worn video. The assessment and final report will review technical effectiveness, legal considerations and usefulness in practice to everyday policing and investigation processes. It will develop a set of standards, protocols, and operational evaluations to provide a base for the development of good practices for body worn video if the evaluations confirm the value of the technology to the policing community. The PIA describes the Edmonton Police Service's assessment to ensure compliance with the *FOIP Act* and the measures taken to protect privacy.

Two additional instruments relevant to the use of BWCs have been considered by the CPS:

Guidance for the Use of Body Worn Cameras by Law Enforcement Authorities

A Matter of Trust: Integrating Privacy and Public Safety in the 21st Century

Both documents have been issued by the Privacy Commissioner of Canada. The *Guidance* document in 2014 has since been endorsed by all of Canada's provincial and territorial privacy oversight offices including the Information and Privacy Commissioner of Alberta. It strongly urges that law enforcement authorities undertake a comprehensive Privacy Impact Assessment when contemplating the use of BWCs. It asserts that BWCs will collect "personal information", and that they are inherently "privacy invasive". The Guidance document highlights particular concerns including:

- Notifying the public
- Continuous versus intermittent recording
- Avoiding recording bystanders
- Proper safeguards, retention, destruction and storage of BWC recordings
- Use of video analytics, and
- Individual Access.

Each of the six concerns identified in the *Guidance* document have been addressed by the CPS.

1. Notification to the Public: CPS has a plan to inform Calgarians generally about the BWC initiative and the features of that initiative to address *FOIP* obligations. In addition, officers will be required to advise individuals when it is safe and practicable to do so that their interaction with officers is being video and audio recorded.

2. No continuous recording: The BWC will be worn by officers throughout their shift; however, the BWC will only be activated when the officer is engaged in law enforcement and policing duties. The BWC will generally not be activated in bathrooms, change rooms, places of worship, lawyer offices unless special circumstances apply such as an emergency call for service originating from such a location.

3. Police officers will be instructed to take all reasonable steps to avoid recording members of the public not subject to a law enforcement investigation.

4. The CPS has comprehensive safeguards to ensure the personal information is protected until it is destroyed in accordance with record retention schedules. The security measures are detailed in Schedule 1 to this PIA.

5. The CPS has no current plans for engaging video analytics in conjunction with the use of BWC or ICDV. The purpose of utilizing BWC and ICDV is to provide additional evidence to support an officer's observations and supplement the notes prepared by an officer.

6. Individual access will be addressed as a request for access under *FOIP*. Individuals will be advised of their right to make an access request. Such requests will be accommodated in accordance with *FOIP*.

The document titled *A Matter of Trust* from November 2010 is an attempt to ensure that in the course of national security and public safety initiatives, there is an appropriate privacy analysis done. It discusses what is a "reasonable expectation of privacy" and outlines four key considerations that should be addressed:

- **Necessity:** There must be a clearly defined necessity for the use of the measure, in relation to a pressing societal concern (in other words, some substantial, imminent problem that the security measure seeks to treat),

- **Proportionality:** That the measure (or specific execution of an invasive power) be carefully targeted and suitably tailored, so as to be viewed as reasonably proportionate to the privacy (or any other rights) of the individual being curtailed,

- **Effectiveness:** That the measure be shown to be empirically effective at treating the issue, and so clearly connected to solving the problem, and finally,

- **Minimal intrusiveness:** That the measure be the least invasive alternative available (in other words, ensure that all other less intrusive avenues of investigation have been exhausted).

In terms of the four element test in the *Matter of Trust* document, the CPS has considered each element in its development of BWC and advises as follows:

Necessity: Public confidence in a municipal police force and its professionalism is essential. An important part of accountability is greater transparency. These values are addressed by the adoption of BWC and the resulting ability to garner additional evidence as to what happened and what was said in any given interaction between an officer and an individual. The BWC is the technology that enables greater transparency and accountability when officers interact with the public. Courts seek the 'best evidence' when dealing with the prosecution of offenders. BWC technology ensures that the best evidence is available to the courts in criminal cases. The use of officer notes and reliance on memory has been the long standing reporting system for police officers. The Braidwood Inquiry in the Robert Dziekanski case in British Columbia highlighted what happens when the memory of the attending officers is seriously flawed. The CPS is not aware of any other technology or process that could accomplish the same business purposes of BWC. ICDV and BWC present a technology that has no comparison.

Proportionality: The CPS has considered how the BWC can be targeted and suitably tailored to be proportional to the privacy of the individual being curtailed. BWC will not be operating when police officers are speaking with members of the public for purposes other than the discharge of their law enforcement and policing duties. BWC of a strip search would not be permitted.

Effectiveness: To ensure the BWC technology is effective the CPS undertook a pilot program between 2012 November 8 and 2013 May 10. It has consulted with and considered the BWC experience of police services in the United Kingdom and United States, and hosted an International Workshop in Calgary to learn from police experience with BWC in other jurisdictions. The traditional practice of officers recording in notebooks their activities and encounters with individuals during a shift will continue but it has limitations in that it is authored by the subject officer. The advantage of a BWC is that this creates an additional and reliable record of the officer-citizen interaction.

Minimal intrusiveness: When it is safe and practicable to do so, all officers are required to advise individuals when the BWC recording is taking place. Due consideration will be given by a member when using a BWC in a residence, a place of worship, in bathrooms and change rooms and when dealing with youth. While the BWC may be invasive in terms of the privacy of individuals, there is no less intrusive avenue to achieve the goals of transparency and accountability as efficiently or effectively as BWC.

These same considerations have been identified in the United Kingdom Information Commissioner Office's Surveillance Code. The Alberta Commissioner and her colleagues in the Guidance document also support these same considerations. It is with these legal

authorities and consideration in mind that the collection, use and disclosure of personal information via BWC and ICDV will be conducted.

C.2 COLLECTION OF PERSONAL INFORMATION

The definition of personal information in s. 1(n) of *FOIP* includes the following:

> 1(n) "personal information" means recorded information about an identifiable individual, including
>
> (i) the individual's name, home or business address or home or business telephone number,
>
> (ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
>
> (iii) the individual's age, sex, marital status or family status,
>
> (iv) an identifying number, symbol or other particular assigned to the individual,
>
> (v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
>
> (vi) information about the individual's health and health care history, including information about a physical or mental disability,
>
> (vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given, [emphasis added]
>
> (viii) anyone else's opinions about the individual
>
> (ix) the individual's personal views or opinions, except if they are about someone else.

During the recording by a BWC or ICDV, the information recorded may include many different elements of personal information and may be captured by the video feature or the audio feature. Due to the nature of how these tools are intended to be used, the precise nature of personal information that may be collected at any given time will vary.

BWC and ICDV are intended to capture actions and conversations which transpire during a police-public interaction for law enforcement reasons. The nature and extent of personal information collected is expected to vary widely across all videos that are recorded, but can be expected to include conversations, actions, behaviors and ambient sounds. The range of information potentially captured by the audio feature includes, but is not limited to:

- Name
- Date of birth
- Home address
- Place of employment
- Specific reasons for the current interaction with police
- Names and contact information of other persons present that are recorded within the capabilities of the BWC or ICDV
- Accents or speech impediments
- Spontaneous or solicited utterances by individuals.

The range of information potentially captured by the video feature includes, but is not limited to:

- Physical characteristics of the individual (e.g. height, weight, eye colour, hair colour, race, ethnic origin)
- Eyeglasses
- Hearing aids
- Scars and facial markings
- Bandages, splints, crutches
- Conspicuous prostheses
- Range of gesticulation and 'body language' of an individual
- Certain kinds of physical impairment
- General demeanor of an individual
- Immediate reactions to things said by an officer(s) or other individuals.

Section 33 and 34 of *FOIP* govern a public body's ability to collect personal information. Section 33 sets out the purposes for which personal information can be collected.

> 33 No personal information may be collected by or for a public body unless
>
> (a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,
>
> (b) that information is collected for the purposes of law enforcement, or
>
> (c) that information relates directly to and is necessary for an operating program or activity of the public body. [emphasis added]

Section 34 addresses the method of collection of personal information. It provides in part that:

34(1) A public body must collect personal information directly from the individual the information is about unless

(a) another method of collection is authorized by (i) that individual, (ii) another Act or a regulation under another Act, or (iii) the Commissioner under section 53(1)(h) of this Act,

(b) the information may be disclosed to the public body under Division 2 of this Part,

(c) the information is collected in a health or safety emergency where (i) the individual is not able to provide the information directly, or (ii) direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or another person,

(d) the information concerns an individual who is designated as a person to be contacted in an emergency or other specified circumstances,

. . .

(g) the information is collected for the purpose of law enforcement,

Law enforcement is defined in *FOIP*.

1(h) "law enforcement" means

(i) policing, including criminal intelligence operations,

(ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or

(iii) proceedings that could lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred;

FOIP provides clear authority for the collection of personal information for law enforcement purposes. The collection of personal information via the use of BWC and ICDV technology has also been endorsed by the courts in Canada. The courts have encouraged police to make evidentiary records of police civilian interactions in a number of settings. For example, police have been encouraged to videotape and audiotape confessions by the Supreme Court of Canada in *R*. v. *Oickle*, [2000] 2 SCR 3 (CanLii) and by the Ontario Court of Appeal in *R*. v. *Moore-McFarlane,* 2001 CanLii 6363. Specifically in *Oickle*, Justice Iacobucci found that

recording confessions assists the trier of fact in assessing the voluntariness and the veracity of the confession, thus guarding against false confessions.

Collection of personal information utilizing BWC and ICDV is primarily designed to assist in law enforcement and policing as well as the preservation of evidence. Accordingly, CPS officers will be instructed to avoid recording uninvolved bystanders or benign interactions with the public, to an extent that is reasonably possible. Where appropriate and where possible, the BWC or ICDV video of third party information will be anonymized before a video is disclosed or released.

In cases where BWC or ICDV video has captured non-involved individuals, authorized CPS *FOIP* Section personnel will use software to blur the faces and mute audio that may identify an individual or contain privileged information. These techniques may be applied when videos are used for internal training purposes, released pursuant to a *FOIP* request, or disclosed to the Crown.

C.3 USE OF PERSONAL INFORMATION

Use of personal information collected through the use of BWCs or ICDV must conform to section 39 of *FOIP*.

> 39(1) A public body may use personal information only
>
> (a) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,
>
> (b) if the individual the information is about has identified the information and consented, in the prescribed manner, to the use, or
>
> (c) for a purpose for which that information may be disclosed to that public body under section 40, 42 or 43.
>
> (4) 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.

With respect to the limitation in s. 39(1) of *FOIP*, the use to which the personal information collected by BWC and ICDV is limited by the purpose for which it was collected, section 39(4) of *FOIP* further limits use to that which is necessary to enable the CPS to carry out its purpose in a reasonable manner.

Section 39(4) of *FOIP* was considered in a law enforcement context by the former Alberta Commissioner. In Order F2006-033 he stated, in part, that:

> Furthermore, it would be unfair to rule on the reasonableness for achieving policing goals of a particular database-searching incident or practice without

giving the [Edmonton Police Service] an opportunity to present evidence and argument in support of what was being done.

In addition, any such analysis would have to take into account that police need to be given space to make both policy and case-by-case decisions about when they need to access information in the database. This is so given the need to rely on intuition and experience, the need to react decisively and quickly in high-pressure situations, and the need to access as much information as possible that is relevant to safety concerns of the members themselves and of the public. [emphasis added]

In the *Report of the Events Relating to Maher Arar* from the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Mr. Justice O'Connor discusses with approval the nature of information collected and used by police forces for law enforcement purposes:

> When an agency such as the RCMP collects information in the course of an investigation, it assumes a type of proprietary interest in and control over that information. The information becomes its work product. The RCMP stores the information in its files or information storage systems and does not routinely make it available to the public. It controls the use to which the information may be put, subject to the requirements of law.
>
> In the interests of conducting thorough investigations, the RCMP collects as much information as possible that may be related to what is being investigated. The inclination of a good investigator is to cast a wide net and, as the investigation proceeds, analyze the information to determine what is useful and what is not. The information gathered may include some of a personal nature about individuals targeted by an investigation or others connected in some way those individuals.
>
> In a normal investigation, the information collected will have varying degrees of value over time. Some may turn out to be irrelevant, unreliable or even inaccurate. In some circumstances, the information may be potentially misleading because it creates an inaccurate or unfair picture about a particular event or individual. [p. 103]

In addition to the law enforcement functions that BWC and ICDV will perform, the CPS will utilize BWC and ICDV video for the following policing functions:

- Education and training of CPS members;
- Internal Professional Standards Section investigations, to augment the evidence used to prove or disprove allegations of unprofessional conduct or misconduct;

- BWC video may be disseminated in the interest of public safety and to maximize public trust and confidence.

Each of these three applications or uses would qualify as a consistent purpose within the meaning of s. 41 of *FOIP*, which provides as follows:

> Consistent purposes
>
> 41 For the purposes of sections 39(1)(a) and 40(1)(c), a use or disclosure of personal information is consistent with the purpose for which the information was collected or compiled if the use or disclosure
>
> (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 or discloses the information.

The utilization of BWC video beyond court disclosure and *FOIP* requests will be controlled and will be subject to prior written approval by the Superintendent in charge of the Field Operations Division and, where warranted, in consultation with the *FOIP* section.

All requests for BWC video, beyond court disclosure and *FOIP* requests, will be made using the CPS Body Worn Camera Request form [attached]. Each request form will be reviewed by the Superintendent Field Operations Division. Approval or denial will be provided in writing. A log of each BWC video request, rationale for decision, and disposition will be maintained by the Superintendent.

If the BWC video request is approved, all material third party information contained within the BWC video will be redacted and edited. This process will mirror the process utilized in response to *FOIP* access requests.

Finally, it is important to note that the CPS is a member of a Provincial BWC Steering Committee. One of the objectives of the committee is to determine if a provincial standard framework can be established about what criteria is required for BWC video to be utilized outside of court disclosure and *FOIP* requests.

The Provincial committee is comprised of:

- Members of the CPS BWC Project Team
- CPS Deputy Chief – Bureau of Community Policing
- CPS Superintendent – Field Operations Division
- Calgary Chief Crown Prosecutor
- Calgary Crown Prosecutors

- CPS Legal Counsel
- Alberta Prosecution Service - Senior Policy Counsel, Edmonton
- Calgary Police Commission
- Edmonton Police Service
- Chief Superintendent RCMP.

The combined effect of the prescribed policies, provincial government direction and relevant statutes is to ensure that the use of personal information obtained for purposes of BWC and ICDV is only to the extent necessary to enable the CPS to carry out its purpose in a reasonable manner.

C.4 DISCLOSURE OF PERSONAL INFORMATION

The key privacy transactions for normal operation of the BWC and ICDV program are collection and use. Disclosure is not a significant issue with respect to the normal use of BWC and ICDV program apart from disclosure to the Crown Prosecutors for purpose of court proceedings. One of the identified risks of such a program, however, is function creep and that might include the prospect that the database created by the BWC or ICDV program is disclosed to other police services, immigration or border security agencies or even to similar agencies outside of Canada.

Disclosure of personal information is addressed in s. 40 of *FOIP* and the most relevant provisions are as follows:

40(1) A public body may disclose personal information only

(a) in accordance with Part 1,

(b) if the disclosure would not be an unreasonable invasion of a third party's personal privacy under section 17,

(c) for the purpose for which the information was collected or compiled or for a use consistent with that purpose,

(d) …

(e) for the purpose of complying with an enactment of Alberta or Canada or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada,

(f) for any purpose in accordance with an enactment of Alberta or Canada that authorizes or requires the disclosure,

(g) for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production

of information or with a rule of court binding in Alberta that relates to the production of information,

. . .

(q) 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,

. . .

(r) 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,

. . .

(ee) if the head of the public body believes, on reasonable grounds, that the disclosure will avert or minimize (i) a risk of harm to the health or safety of a minor, or (ii) an imminent danger to the health or safety of any person,

. . .

(gg) to a law enforcement agency, an organization providing services to a minor, another public body or any prescribed person or body if the information is in respect of a minor or a parent or guardian of a minor and the head of the public body believes, on reasonable grounds, that the disclosure is in the best interests of that minor.

(4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) in a reasonable manner.

A public body is also obliged by s. 38 of *FOIP* to:

> "protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction"

Section 39(4) and its limitation on use by a public body has a counterpart for disclosure in section 40(4) that:

> 40(4) A public body may disclose personal information only to the extent necessary to enable the public body to carry out the purposes described in subsections (1), (2) and (3) <u>in a reasonable manner</u>. [emphasis added]

We are mindful of the provisions for disclosure, without consent, to other law enforcement agencies in s. 40(1)(q) and (r) of *FOIP*.

> 40(1) A public body may disclose personal information only
>
> . . .
>
> (q) 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,
>
> (r) 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.

In the event that a request came to CPS from another law enforcement agency, it would only be considered in compliance with the above subsections of s. 40 of *FOIP*. In addition, the CPS would be constrained by the *Charter of Rights and Freedoms* (sections 7 and 8) and by the specific recommendations for sharing of personal information between law enforcement agencies from Mr. Justice O'Connor in the *Report of the Events Relating to Maher Arar*.

C.5 ACCESS AND CORRECTION REQUESTS

Access requests will be routed through the CPS *FOIP* Section, following current practices of requests for information. The CPS website provides all of the information required to make a *FOIP* request. Access requests are assigned to a Disclosure Analyst who communicates with the applicant to confirm and clarify the request, if required. The Disclosure Analyst then provides the responsive records or alternate response pursuant to our obligations under *FOIP*.

The recorded video is intended to be an accurate, real time, account of what transpired during a police-public interaction; therefore, correction requests are not directly applicable – as the video will remain unaltered. In the event that an individual asserts that the video is not a true representation of an event because the BWC was turned off for a time, that individual can seek to have a notation made in accordance with s. 36(3).

If incorrect information was transcribed from the video into a police records management system, there is a process for editing the report to correct the information. A log of all data edits is maintained.

C.6 ADDITIONAL FORMS OF ACCOUNTABILITY FOR CPS

Police services in Alberta are not only accountable under *FOIP* for personal information they collect, use and disclose. In addition to complying with *FOIP*, CPS must also comply with other federal and provincial statutes, including but not limited to the *Youth Justice Act*, R.S.A. 2000, c. Y-1, the *Child Youth and Family Enhancement Act*, R.S.A. 2000, c. C-12, the *Children First* Act, S.A. 2013, c. C-12.5, the *Police Act*, R.S.A. 2000, c. P-17 and the Federal *Youth Criminal Justice Act*, S.C. 2002, c.1, *Criminal Code of Canada*, R.S.C. 1985, c. C-46 and the Canadian *Charter of Rights and Freedoms*.

The *Police Act* provides a good example of the additional legislation, over and above *FOIP*, that governs the CPS and ensures proper protection of personal information collected as part of the law enforcement and policing functions carried out by CPS members. Section 38(1) of the *Police Act* describes the general duties and authority of all police officers in the Province of Alberta:

> 38(1) Every police officer is a peace officer and has the authority, responsibility and duty
>
> a. to perform all duties that are necessary
>
> (i) to carry out the police officer's functions as a peace officer,
>
> (ii) to encourage and assist the community in preventing crime,
>
> (iii) to encourage and foster a co-operative relationship between the police service and the members of the community, and
>
> (iv) to apprehend persons who may lawfully be taken into custody, and
>
> b. to execute all warrants and perform all related duties and services.

The Police Service Regulation (Alberta Regulation 356/90) sets out the activities that constitute misconduct. It states:

> 5(1) A police officer shall not engage in any action that constitutes one or more of the following:
>
> (a) breach of confidence;
>
> . . .

(2) For the purposes of subsection (1),

(a) "breach of confidence" consists of one or more of the following:

(i) divulging any matter that it is his duty to keep in confidence;

(ii) giving notice, directly or indirectly, to any person against whom any warrant or summons has been or is about to be issued, except in the lawful execution of the warrant or service of the summons;

(iii) without proper authorization from a superior police officer or in contravention of any rules of the police service of which he is a member, communicating to the news media or to any unauthorized person any matter connected with the police service;

(iv) without proper authorization from a superior police officer showing to

(A) any person who is not a member of the police service, or

(B) any unauthorized member of the police service, any record that is the property of or in the custody of the police service;

(v) signing or circulating a petition or statement in respect of a matter concerning the police service, except through the proper official channel or correspondence or established grievance procedure.

The CPS also has a common law duty to protect the privacy of police informants and confidential sources and pursuant to s. 3.1 of the Alberta *Police Act* police officers must follow the direction of the Alberta Minister of Justice and Solicitor General as published in the *Alberta Provincial Policing Standards Manual*.

In addition to being accountable to the Office of the Information and Privacy Commissioner, CPS is also accountable to the courts and to the Law Enforcement Review Board should there be any violations with respect to the collection, use or disclosure of personal information as a result of the use of BWC or ICDV.

C.7 NOTICE

BWC and ICDV is a tool used to overtly assist in obtaining evidence at the scenes of incidents and crimes dispatched or on-view calls for service as well as traffic stops. The public awareness campaign associated with the implementation of BWCs will ensure that the public is generally aware that police officers are wearing BWCs and will be recording interactions with the public. If a member of the public inquires, an officer will advise if a recording is being conducted. To further ensure awareness of video recording, members recording via a BWC or ICDV, shall, when it is practicable and safe to do so, announce that

the interaction is being recorded. This notification will generally be accomplished by pointing at the BWC or ICDV microphone and stating audibly that the interaction is being recorded.

No Reasonable Expectation of Privacy

It is important to note that generally speaking there is no reasonable expectation of privacy in the context of an interaction with a police officer. The fact that the public ought not to have a reasonable expectation of privacy when interacting with police officers was recognized in the decision of *R*. v. *Tuck*, 2009 CanLii 83172 (OJN SC). The accused was a suspect in a homicide. In the course of their investigation, police interviewed the accused on several occasions. The accused asked Detectives to not make recordings of the conversations and the officer assured him he would only take hand written notes. Several of the conversations were surreptitiously recorded. At trial the accused sought to exclude the conversations arguing that the recordings were made without statement consent or a judicial authorization, therefore an unreasonable search and seizure and a Section 8 violation. The Crown's position was that there could be no reasonable expectation of privacy in the communications between the Detective and the accused. Accordingly, no Section 8 breach existed. Alternatively, if there was a breach, it was a technical breach on a point of law that was, and is, unclear. Ultimately the Trial Judge agreed with the Crown and stated at para. 35 of the decision:

> "The reasonable expectation of privacy in a conversation with a police officer has been considered in two cases in this court. Ferguson J. in *R. v. S.S.*, found that anyone who speaks to police engaged in the execution of their duty should be taken to assume that his or her words will be preserved and used by the state. The preservation would at least involve taking notes. Ferguson J. concluded that in such circumstances there is no reasonable expectation of privacy. Abbey J. reached the same conclusion in *R*. v. *Jenkins*."

Communication Strategy

In order to ensure that the public is aware that, generally speaking, they should not have an expectation of privacy when they interact with a police officer a robust communication strategy will be launched as part of the BWC program. The primary objective of the communication strategy will be to advise members of the public that they should expect to be recorded anytime they interact with a CPS officer.

As part of the communications strategy, the CPS will be releasing the BWC policy, this Privacy Impact Assessment (PIA) and Responses to the Privacy Commissioner to the public via the CPS website. The BWC rollout, CPS policy and the BWC PIA will be publicized through a public consultation strategy (currently under development by CPS Public Affairs).

This strategy is anticipated to include:

- Media liaison meeting will be held prior to the roll out to ensure media have a thorough understanding of the policy and disclosure process;
- Joint open house for the public hosted by Calgary Police Commission and Calgary Police Service at initial roll out of cameras;
- Subsequent open houses in each district or quadrant of the city when body worn cameras are rolled out in that specific area. The District office as well as the body worn camera project team would lead these open houses to ensure that issues specific to each community form part of the discussion;
- Webpage on Calgarypolice.ca that includes the policy, privacy impact assessment, and frequently asked questions section;
- Articles in community association newsletters that can also be distributed to members of Council to include in their monthly newsletters;
- Public survey to be compiled by the CPS Strategic Services Division;
- A paid advertising campaign that includes:
    - Digital advertising with three daily newspapers – Metro, Calgary Herald, Calgary Sun;
    - Transit advertising for minimum one-month period. Includes interior as well as exterior bus shelters/transit platforms;
    - 'Report to Calgarians' television segment.

The goal of this strategy is to engage the public in a thoughtful discussion and understanding of CPS commitment to public safety, transparency and officer integrity.

C.8 DATA MATCHING

This data differs from a traditional database in that there are no discrete data fields available for users to perform routine database searches. Rather, searches will be reliant on the metadata and any keywords or tagging added by end-users. As such, it is more likely that these files will be searched by date/time or police event number, rather than specific personal or private information.

When the content of the video will be used for evidentiary purposes, it will be linked to an existing police investigation or charging document – such as an occurrence report or summons. When no such relationship exists, the video will be tagged with the reference from the original call for service and stored securely as described throughout this document.

C.9 USE OF PERSONAL INFORMATION OUTSIDE ALBERTA

In the event that CPS is contemplating an arrangement that involves the transfer of personal information in either the BWC or ICDV databases outside of Alberta, the CPS would consider the elements detailed in s. 8(4) of the *Health Information Regulation* 70/2001 and how to integrate those elements in any out-sourcing contract.

C.10 RETENTION

All information collected by the CPS, including personal information, is subject to the Calgary Police Service Records Retention Schedule and the Records and Information Management Policy - Ref #MR-010. Data Retention periods are established by each operational unit based on the business needs of the Service.

Alberta Policing Standards, which are prescribed by the Director of Law Enforcement, mandates Alberta police agencies that have holding or detention facilities, to retain that video for 13 months. Retention periods for other investigative videos are determined by CPS policy and are dependent upon the type of offence and the nature of the investigation.

The following CPS retention schedules and their respective offences:

- Citizen Contact: 13 months
- Enforcement Activity: 13 months
- Domestic – Charges: 40 years
- Domestic – No Charges: 13 months
- Drugs – Charges: 40 years
- Drugs – No Charges: 13 months
- Criminal Code Charges – Other: 40 years
- Criminal Code Offense – No Charges: 13 months
- Traffic – Criminal Code Charges: 40 years
- Traffic – Other: 10 years
- Ticket/Summons: 13 months
- Homicide: Indefinite
- Sexual Assault: Indefinite
- Child Abuse Investigations: Indefinite
- Major Incident – Other: Indefinite

SECTION D - PRIVACY RISK MITIGATION

D.1 ACCESS CONTROLS

The ICDV and BWC project team consulted with both the *FOIP* Section and IT Section about access controls.

Access to the videos will be consistent with the "need-to-know" principle. Files will be transferred directly from the recording device to the CPS network at the end of each shift. This transfer process is automated, and will be managed by software. Further, once the video is on the CPS network, the same back-end software will maintain a complete audit history of access to, viewing of, and modifications or edits to each video file.

Video storage systems are controlled using a Role Based Access Control (RBAC).

D.2 PRIVACY RISK ASSESSMENT AND MITIGATION PLANS

Based on the experience of the OIPC, five broad risk categories were identified as relevant to most projects. Those risks and their potential mitigation measures are described in the table below.

Privacy Risk	Description	Mitigation Measures	CPS Policy Reference
Unauthorized use of information by authorized users	There is potential for authorized users to share or otherwise make public unauthorized copies of their videos, in whole or in part. This can be achieved through direct or indirect means. For example: using a personal Smartphone to record a copy of the video as it plays on CPS equipment, effectively bypassing the encryption and security features inherent to this project.	The actions described would be a clear breach of CPS policy and dealt with appropriate discipline. Training with respect to these expectations will be reinforced when the cameras are first issued.	Information Technology Policy and *FOIP* Policy
Unauthorized collection/use or disclosure of information by external parties	Not applicable.	External parties will not have access to the CPS network where these files are stored. External parties under an MOU which does grant access	In the case of disclosure, the Defence/Accused signs an undertaking to not release

		to the CPS network will not be able to log into the video management software.	
Unauthorized collection/use or disclosure of information by external parties	Not applicable.	External parties will not have access to the CPS network where these files are stored. External parties under an MOU which does grant access to the CPS network will not be able to log into the video management software.	In the case of disclosure, the Defence/ Accused signs an undertaking to not release
Loss, destruction or loss of use of information	Occasionally, the BWC or ICDV may malfunction or be damaged prior to transferring the video to the CPS network.	The videos are intended to be only one facet of any police-public interaction or investigation. Officers wearing BWCs will also be expected to maintain "officer notes". Depending on the nature of the malfunction or camera damage, recovery of any video may be possible by specially trained technicians.	Records Management and Information Policy
Loss of integrity of information	Not applicable.	Not applicable	
Unauthorized or inappropriate collection/use or disclosure by a contractor or business partner			Information Technology Policy and *FOIP* Policy as well as contractual requirements

The BWC and ICDV have multiple security safeguards to prevent tampering and unauthorized access. Significantly, the BWC and ICDV do not utilize cloud storage. The CPS retains custody and control of all personal information captured by the BWC and ICDV systems.

Schedule 1 to this PIA is the discussion of the Security Safeguards of the BWC and ICDV. This schedule will not be made publicly available, since it would compromise the security of the personal information captured by the BWC and ICDV systems.

The CPS BWC policy is in the process of being finalized. Upon finalization of the BWC policy, all members of the CPS will be trained to the policy.

The CPS Chief Crowfoot Learning Centre is in the final stages of completing a curriculum for all CPS officers that are to be issued a BWC. A BWC will not be issued until the Learning Centre designated 16 hour course has been completed.

The general premise for the use of BWC is:

- When considering the use of a BWC, the law enforcement objective must be weighed against privacy concerns, to ensure an appropriate balance between policing needs and privacy rights.

The Learning Centre BWC instruction course is tentatively outlined as follows:

- Introduction;
- Benefits of using BWCs;
- Privacy considerations and a review of privacy law, *FOIP*;
- Limitations of BWCs;
- Technical features;
- How to put on a BWC;
- How to use the docking station;
- Equipment and data storage;
- CPS policy on BWC:
    - Use of a BWC;
    - Activation and Deactivation;
    - Prohibitions;
    - Misconduct;
    - Reporting and Disclosure.

The CPS has a Departure from Service Checklist for CPS members who have either resigned, retired, or have been terminated from employment with the CPS. The checklist contains a section for the CPS ICTS to verify that the outgoing employee has returned all laptops, flash drives, and remote access tokens. The checklist also contains a section to verify that all CPS electronic accounts have been de-activated, this de-activation is done to correspond to the CPS member's departure date. Only once the CPS Human Resource Operations Section has received the completed checklist from the employee will the CPS Finance Section process the departing member's final pay.

All CPS members retain their own individual access to the secure BWC software program no matter where in the organization they are currently deployed. When the retention period of a BWC recording is reached, it will be removed automatically from the server by the BWC software. The storage system will note the deletion and mark the storage media for recycling. The media will be automatically erased and overwritten with new incoming BWC video, preventing retrieval of old information.

The media itself is re-used until it is no longer serviceable. At that point, the media will be physically destroyed by use of a degausser (a device that uses strong magnetic fields to erase magnetic storage media so that the data is irretrievably destroyed), and then shredding.

D.3 MONITORING

The CPS BWC Coordinator is responsible for:

- managing BWC recordings;
- being the primary CPS contact for the training, maintenance, and use of the BWC system;
- being under the direction of the Superintendent of Field Operations, the BWC Coordinator administers and manages access and security to BWC recordings;
- managing requests for BWC recordings that are submitted for criminal investigations of CPS officers;
- allocating, issuing, replacing, tracking, and trouble-shooting the BWC devices, docking stations and software;
- maintaining a log of BWC assignments;
- obtaining the written approval of the CPS Superintendent, Field Operations Division to release any video not required as part of disclosure;
- assisting the CPS Manager, *FOIP* Section with *FOIP* requests.

Although CPS officers will be able to upload, view and review their own BWC video as is necessary during the performance of their duties, only the CPS BWC Coordinator and three members of the Court & Disclosure Unit will be able to export and download BWC video.

One feature of the BWC system is a continuity log that will document all transactions pertaining to every BWC video. The system will log all activity from the time the file is recorded to the time it is downloaded into the storage facility. This creates an entry on a continuity log that is traceable to the individual CPS officer, BWC and BWC video. Any time a BWC video is reviewed, tagged or transferred in any manner, an entry is generated in the continuity log. The continuity log cannot be edited or manipulated, even by those with the highest level of access.

An audit schedule for the regular and ongoing review of the BWC and ICDV systems will be set out in the applicable policies.

D.4 PIA COMPLIANCE

This PIA is accurate as of September 8, 2015. Any material modifications made to the project may require revisions to this PIA to ensure that it remains current and accurate. It will be the responsibility of the Privacy Counsel and Manager, *FOIP* Section, to monitor the need for revisions to the PIA and to advise the Chief of Police accordingly.