


HAMILTON POLICE SERVICE BOARD

RECOMMENDATION REPORT



TO:	Chair and Members Hamilton Police Service Board
BOARD MEETING DATE:	September 26, 2024
SUBJECT:	Draft Board Policy on the Use of Body-Worn Cameras
REPORT NUMBER:	PSB 24-029
SUBMITTED BY:	Kirsten Stevenson, Administrative Director
SIGNATURE:	

RECOMMENDATION

That the draft Board Policy on the Use of Body-Worn Cameras as attached to this report be approved.

EXECUTIVE SUMMARY

- The Board approved the purchase of body-worn cameras at their June 27, 2024 meeting
- At their August 1, 2024 meeting, the Board directed the Administrative Director to prepare a draft Board policy on the use of body-worn cameras in consultation with members of the Service

FINANCIAL – STAFFING – LEGAL IMPLICATIONS

Financial: not applicable

Staffing: not applicable

Legal Implications: not applicable

INFORMATION

The rollout of a body-worn program and creation of Board policy aligns with the Board's Strategic Plan to leverage technology and innovation, with the goal of modernizing the Hamilton Police Service. The aim is to increase transparency and accountability in public interactions while enhancing public and officer safety.

Vision: To be a trusted partner in delivering public safety.

Mission: To serve and protect in partnership with our communities.

Our Values: Compassionate, Dedicated, Inclusive, Integrity, Innovative, Professional, Teamwork

Body-worn cameras (BWCs) have been advanced as one method to increase transparency, enhance accountability for rights protections and situations in which force is used during an interaction with police, and improve law enforcement practices by identifying where a need may exist for additional training, supervision or discipline. BWCs are an effective tool for gathering evidence and providing a more accurate record of events, which assists in improving the work of the criminal justice system as a whole.

The Administrative Director (A.D.) worked in collaboration with Sergeant Scott Moore (HPS Strategic Initiatives), Manager of HPS Records, Property and Evidence Anne Hepplewhite as well as other members of the service, to prepare this draft policy for the Board's consideration.

When preparing the Board's draft policy, and in considering best practices, the following resources were reviewed and taken into consideration:

- The Information and Privacy Commission of Ontario's 'Model Governance Framework for Police Body-Worn Camera Programs in Ontario Guide (June 2021);
- Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities (developed by the Office of the Privacy Commissioner of Canada in collaboration and consultation with multiple provincial privacy oversight offices);
- Current Big 12 Police Service Board policies on BWCs.

The Board's Legal Advisor reviewed the draft policy to ensure consistency with the above-noted guidance documents.

The Board's Policy on BWCs adheres to the 'Model Governance Framework for Police Body-Worn Camera Programs in Ontario Guide' as noted above; in doing so, the Board's BWC Policy complies with Ontario's access and privacy laws and also assists the Board in establishing the necessary checks and balances to carry out their important oversight role. The Framework, as well as Board Policy, outlines the key transparency, accountability, privacy and access consideration for a success BWC program. They also ensure compliance with Board obligations under the Ontario's access and privacy laws.

The draft policy is broken out into 4 main areas. These areas and sub-areas provide thorough policy coverage of matters relating to the effective governance of BWCs, specifically with reference to ensuring public privacy is made a priority during the use of BWCs:

- Guiding Principles
- Purpose of the Policy
- Risks and Mitigation
- Main Policy
 - General
 - When and How to Use Body-Worn Cameras

Vision: To be a trusted partner in delivering public safety.

Mission: To serve and protect in partnership with our communities.

Our Values: Compassionate, Dedicated, Inclusive, Integrity, Innovative, Professional, Teamwork

- Controls
- Transparency
- Secure Retention and Disposal of Recordings
- Limited Use and Access to Body-Worn Camera Recordings
- Auditing
- Reporting
- Board Review of Policy

ALTERNATIVES FOR CONSIDERATION

The Board may wish to defer approval of the draft Board Policy on Body-Worn Cameras to a future date.

APPENDICES ATTACHED

Appendix 'A' – Draft Board Policy on the Use of Body-Worn Cameras

Appendix 'B' – Model Governance Framework for Policy Body-worn Camera Programs in Ontario (June 2021 – Information and Privacy Commissioner of Ontario)

Appendix 'C' – Guidance for the Use of Body-worn Cameras by Law Enforcement Authorities (developed by the Office of the Privacy Commissioner of Canada in collaboration with privacy oversight offices across Canada)

Vision: To be a trusted partner in delivering public safety.

Mission: To serve and protect in partnership with our communities.

Our Values: Compassionate, Dedicated, Inclusive, Integrity, Innovative, Professional, Teamwork



Hamilton Police Service Board Use of Body-Worn Cameras Policy P-025

Effective date:
Reviewed:
Amended:

Applicable Legislation

Municipal Freedom of Information and the Protection of Privacy Act, R.S.O. 1990, and
Community Safety and Policing Act, 2019, S.O. 2019, c.1, Sched.1 (*the Act*):

Guiding Principles

The Hamilton Police Service Board (the Board) is committed to providing fair, effective, efficient, equitable and accountable policing to the members of our communities, in accordance with the fundamental rights guaranteed by the *Charter of Rights and Freedoms* and the *Human Rights Code* of Ontario. The Board is also committed to ensuring the inherent worth and dignity of all individuals who come into contact with police is respected in all interactions.

By recording interactions with members of the public and the police, body-worn cameras (BWCs) have been advanced as one way to increase transparency, enhance accountability for rights protections and situations in which force is used and these recordings may also improve law enforcement practices by identifying where a need may exist for additional training, supervision or discipline. BWCs will also enable the timely and fair investigation of any allegations of misconduct by Service Members, and a quick resolution of complaints.

BWCs are effective tools for gathering evidence and providing a more accurate and robust record of events, thus improving the work of the criminal justice system as a whole.

Purpose of Policy

The purpose of this Policy is to direct the Chief to authorize the Service to deploy and use BWCs and to ensure their use by the Service occurs in such a way as to ensure the following public interests are served:

- Improving the transparency of the Service with regards to allegations of discreditable conduct, improper conduct, misconduct, biased service delivery and excessive or improper use of force by Service Members;
- Ensuring the accountability of the Service and Service Members through internal and public oversight systems;
- Protecting individuals' right to privacy by limiting access to recordings from BWCs to the greatest extent possible and to as limited a number of people as possible;
- Ensuring individuals have access to their personal information when it is collected by the BWCs;
- Enhancing public trust and police legitimacy;
- Enhancing public and police officer safety;
- Enhancing the Service's commitment to anti-racist, bias-free service delivery;
- Providing improved evidence for investigative, judicial and oversight purposes;
- Ensuring timely and fair response to misconduct allegations against Service Members, in a manner that enhances public and Member confidence in the Service's complaint process; and
- Providing information as to the effectiveness of Service procedures and training.

Risks and Mitigation

The Board acknowledges the use of BWCs is not without challenges. There are important concerns surrounding privacy, particularly where what could be perceived as surveillance of vulnerable people and racialized communities is concerned, or in sensitive situations such as domestic violence calls.

The Board recognizes that individuals have a justified expectation of privacy as they go about their daily business, even within public spaces, and this expectation must be respected subject to reasonable limits.

In addition, the manner in which BWC use is implemented and governed could have a substantial impact on their effectiveness as it relates to cases of excessive use of force or other matters that may engage the police oversight system. Similarly, access to recordings must also be strictly governed, both to prevent breach of privacy by internal and external individuals, and to ensure all recordings are preserved in their full, unedited form on the system, throughout their retention period. Finally, the transparency of the implementation of this Policy by the Service, including public access to information on its effectiveness in achieving the Policy's goals is a critical element of building the public trust necessary for the achievement of the Policy's purposes and goals.

The Board will monitor the Service's implementation of this Policy to mitigate these risks, including the provision of robust training to Service Members to ensure the effective deployment of this tool. The Board will also continue to monitor best practices and recommendations to identify possible revisions to this Policy and work with the Service, other emergency services, technology partners and the community to identify other opportunities and strategies to achieve the crucial goals of delivering professional policing in a manner that respects the dignity, privacy, worth and human rights of individuals.

Policy of the Board

It is the Policy of the Hamilton Police Service Board that the Chief of Police, in consideration of information provided by the Information and Privacy Commissioner of Ontario and other relevant stakeholders, will develop procedures that:

General

1. Implement the recommendations set out in the Office of the Privacy Commissioner of Canada's *Guidance for the Use of Body-Worn Cameras by Law Enforcement Authorities* (2015), and ensure new recommendations and best practices continue to be monitored and implemented as they are identified by the relevant provincial and federal authorities.
2. Specifically identify the legislative authority for the collection of personal information that will be captured by the BWCs and ensure any such collection aligns with that authority and all other relevant legislation, including any legislative provisions addressing data, information or records storage, access, use and/or disclosure.
3. Ensure all use of BWCs and their recordings is consistent with the *Ontario Human Rights Code* and the *Charter of Rights and Freedoms*.

When and How to Use Body-Worn Cameras

4. Ensure clear direction in the policies and procedures of who shall be equipped with BWCs and when the cameras shall be activated.
5. Provide guidance to officers on when a BWC must be activated, unless an unexpected and immediate threat to the life or safety of the Service Members or a member of the public makes it impossible or dangerous to activate the BWC prior to that interaction.

6. Establish within the policies and procedures that BWCs will not be used for general surveillance of members of the public.
7. Ensure that clear direction is established within policies and procedures regarding when a Service Member can and cannot deactivate the BWC.
8. Ensure that clear guidelines are established within the policies and procedures governing Service Members from intentionally preventing the BWC from capturing video or audio during an interaction with a member of the public, with the sole exception of temporarily covering the lens to protect the dignity of an individual during situations of a sensitive nature.
9. Establish that Service Members must inform members of the public that are part of an interaction involving BWCs they are being recorded at the earliest opportunity and that the camera is active and recording.
10. Ensure clear guidelines are established within the policies and procedures addressing privacy considerations in situations where there is a heightened reasonable expectation of privacy.
11. Establish, with regards to the BWC's 'stealth mode' (i.e., a mode wherein the BWC is recording without providing visible and audible signals) that:
 - a. The 'stealth mode' will only be used in situations where activating the camera in its normal mode may endanger the safety of a Service Member, and only for the duration necessary for this purpose;
 - b. If a BWC was set to 'stealth mode' prior to an interaction with a member of the public to protect the safety of a Service Member(s), and the Service Member subsequently engages with a member of the public, the Service Member must inform that individual or individuals as soon as reasonably possible that the BWC is activated, and turn off the 'stealth mode' as soon as possible.
12. Establish that Service Members must upload all recordings from the BWC at the end of their shift, and that supervisors must ensure all recordings from BWCs used by Service Members under their supervision have been uploaded.

Controls

13. Establish that if a Service Member has not recorded in full or in part an interaction with a member of the public, the Service Member must document the specific reason a recording was not made in part or in full using a designated process, and that this process must include a review by a Service Member designated by the Chief of Police.
14. Establish training requirements for Service Members to fulfill prior to being issued a BWC, and subsequent on-going training requirements, so as to ensure Service Members are able to comply in full with this Policy.
15. Establish a comprehensive auditing schedule to govern and ensure compliance with policies and procedures.
16. Establish the framework for discipline of Service Members who fail to comply with the policies and procedures governing BWCs.

Transparency

17. Ensure clear and current instructions are posted on the Service's public website providing direction for the public on how to obtain information, details, reports and guidance on the use of BWCs.

Secure Retention and Disposal of Recordings

18. In consideration of information provided by the Information and Privacy Commissioner of Ontario, and in accordance with all applicable legislation, establish and ensure recordings from BWCs, including any meta-data produced by the BWCs or the technology supporting the Service's BWCs, will be:
 - a. Stored on a secure Canadian storage server in accordance with all applicable provincial and federal legislation and security best practices, so as to prevent any editing, tampering and unauthorized access to recordings and meta-data;

- b. Encrypted within the camera during transit to the storage server and while in storage; and
 - c. Destroyed at the end of their retention period in a secure manner which prevents recovery and unauthorized access to the recordings and meta-data.
19. In consideration of information provided by the Information and Privacy Commissioner of Ontario, and in accordance with all applicable legislation, establish the minimum retention period for recordings from BWCs, and conditions for extensions of the retention period.
20. Establish actions to be taken by the Service in the case of a potential or actual access breach of the Service's recording and meta-data storage service, including breach mitigation and control steps, and the steps required to notify the public and impacted individuals of the potential breach.
21. Establish that the Information and Privacy Commissioner of Ontario must be notified as soon as reasonably possible of significant privacy breaches, to be determined through consideration of all relevant circumstances, including whether:
- a. The personal information at issue is sensitive, either by its nature or given its context;
 - b. The breach is likely to cause significant harm, including financial, reputational, or emotional harm, such as embarrassment or humiliation;
 - c. The breach involves the personal information of a large number of individuals;
 - d. The likelihood the personal information at issue could be misused, or further disseminated by others; or
 - e. The Service is having difficulties containing the breach.

Limited Use and Access to Body-Worn Camera Recordings

22. Establish the conditions under which specified individuals may view or receive copies of recordings from BWCs, ensuring that:
 - a. Service Members who wore the BWC which captured a recording may access the recording and make additions to their notes based on the review of the recordings, which must be clearly marked as such, once they have completed any required initial reports, statements and interviews regarding the recorded events;
 - b. Access to recordings by other Service Members is limited only to those with a specified role in relation to the recording which justifies and necessitates such access, including, but not limited to, investigation, supervision, legal proceedings, training development, reporting, and auditing, and will be granted only when circumstances require such access;
 - c. Access to recordings is provided in a timely manner to members of bodies responsible for independent oversight of police (e.g. the Law Enforcement Complaints Agency and the Special Investigations Unit) who are conducting an investigation and who have grounds to believe the recording includes evidentiary materials;
 - d. Access to recordings is provided in a timely manner to individuals who have lawful authority to obtain such access.
23. Establish, notwithstanding the provisions of section 22 of this Policy, additional safeguards to enhance the storage and limit the access to recordings of minors who are suspected of an offence or are witnesses to a suspected offence, in accordance with the *Youth Criminal Justice Act*.
24. Establish an audit trail will be created and maintained by the Service for records that have been requested.
25. Establish that a member of the public may request to view recordings from a BWC or that the recordings and/or their meta-data be released to the requestor.

26. Establish that the Service may only use recordings from BWCs for the purposes of training after the identities of all members of the public captured in the recordings are concealed through measures such as image blurring and voice distortion.

In addition, it is the Policy of the Board that:

27. The Chief of Police may initiate release to the public of recordings from BWCs, taking into consideration relevant factors, including what is consistent with the law and public interest, and what is reasonable in the circumstances of the case. The Chief of Police will include, along with the release, a justification of the public interest in releasing the recording. These releases will be in the Chief of Police's purview as per the CSPA versus an MFIPPA release.
28. Whenever the Chief of Police initiates the release to the public of any recordings from BWCs that include images or voice recordings of members of the public:
 - a. The identities of all members of the public captured in the recordings are concealed through measures such as image blurring and voice distortion, unless the Service is required by law to release the recordings in another form; and
 - b. The Chief of Police will include, along with the release, a justification of the public interest in releasing the recording.

Furthermore, it is the Policy of the Board that the Chief of Police will ensure:

29. Recordings from BWCs will not be used in combination with facial-recognition technology, video analytics software, voice recognition software, or to generate a searchable database of images of individuals who have interacted with Service Members, with the exception of comparing images that are directly related to an investigation to a "mug shot" database in a manner approved by the Board.
30. The Service will not use BWC recordings recorded during a protest in combination with the Service's "mug shot" database unless there are reasonable grounds to believe an offence has been committed at the protest, and then, only

for the purpose of investigating such an offence and comparing only images of the individual suspected of the offence to the images in the database.

31. The Service will conduct a Privacy Impact Assessment in consultation with the Information and Privacy Commissioner of Ontario, and bring its findings before the Board for its consideration *prior* to implementing any significant changes to the Service's use of BWCs, including when:
 - a. The Service wishes to utilize recordings from BWCs in a novel manner or in combination with other software or hardware;
 - b. The technology used to capture, retain, store or destroy the recordings changes beyond routine software updates issued by the supplier, including the deployment of any new or additional features; or
 - c. The scope or governance of the Service's BWC program changes.

Auditing

It is also the Policy of the Board that the Chief of Police will:

32. Ensure the Service conducts an annual audit:
 - a. That reviews BWC recordings and meta-data for:
 - i. all incidents for which a complaint under the *Community Safety and Policing Act* was filed during the reporting period;
 - ii. all incidents for which an investigation was initiated by the Special Investigations Unit or the Law Enforcement Complaints Agency;
 - iii. a sample of incidents for which a Use of Force form was completed during the reporting period;
 - iv. a sample of incidents during the reporting period that were initiated by a call for service;

- v. a sample of incidents during the reporting period that were not initiated by a call for service;
 - vi. all incidents wherein a BWC was disabled for the purpose of protecting law enforcement strategies.
 - vii. a sample of the meta-data for incidents whose retention period has expired during the reporting period.
- b. Ensure the audit includes a review of BWC recordings for these incidents to ensure that:
- i. the recording begins prior to the beginning of the interaction with the member of the public, and if not, that a satisfactory explanation for the failure to activate the BWC before the interaction began was provided in accordance with the Service's Procedure;
 - ii. the subject of the recording is informed at the earliest opportunity in the interaction that the interaction is being recorded for video and audio;
 - iii. any obstruction of the lens or gaps in the recording are justified and of reasonable duration;
 - iv. the recording ends:
 - after conditions for an exception in accordance with section 7 of this Policy have been established; or
 - after the interaction has ended;
 - v. all access to the recordings was justified and necessary;
 - vi. all requests for recordings from the Special Investigations Unit or the Law Enforcement Complaints Agency were fulfilled in full and in a timely manner; and
 - vii. the Service is in compliance with required retention and destruction practices.

33. Advise and file with the Board's' Administrative Director a new copy of the Service's procedure governing BWC use whenever a change is made to the procedure;

Reporting

34. Provide the Board with an annual report which will include:
 - a. A summary of any changes to the relevant procedure(s) made in accordance with this Policy over the reporting period;
 - b. The findings of the annual audit;
 - c. The number of complaints received by the Service with regards to the use or failure to use of BWCs, a summary of the complaints, and a summary of the dispositions of the complaints during the reporting period;
 - d. The total number of complaints received by the Service against Service Members for which there was a relevant BWC recording, broken down by complaint resolution status;
 - e. The number, if any, of recordings requested by the Special Investigations Unit, or the Law Enforcement Complaints Agency, which were not fulfilled within 30 days;
 - f. The number of requests made by members of the public to view or release to the public recordings from BWCs which were refused, if any, and a high-level overview of the reasons for any refusals;
 - g. The total number of recordings currently stored by the Service beyond the default retention period, generally categorized by the reason for the extended retention period;
 - h. The total number of recordings released as part of a disclosure process in a legal proceeding;

- i. The number of reports submitted in accordance with section 13 of this Policy, documenting the reason for a failure to activate the BWC prior to the beginning of an interaction with a member of the public, and the number of these incidents, if any, which were found not be in compliance with the procedure;
- j. The number of Service Members disciplined for lack of compliance with BWC policies and/or procedures and a summary of the disciplinary measures used;
- k. The number of investigations into potential privacy breaches during the reporting period and the number of such incidents that were determined to constitute a breach and a summary description of these incidents.
- l. The costs and/or savings associated with the deployment and use of BWCs in the previous year; and
- m. A review of whether the deployment of BWCs is achieving the purposes set by this Policy, whether their use remains justified in light of these purposes, and whether their use has resulted in any unintended negative impacts, including, but not limited to:
 - i. Use of Force trends over the past five years;
 - ii. complaint trends over the past five years;
 - iii. findings from a survey of public trust in the Service at a timeframe to be determined after a satisfactory implementation period; and
 - iv. findings from a consultation with impacted and marginalized communities.

It is also the Policy of the Board that:

- 35. The Board will review this Policy within one year after full deployment of the BWCs by the Service, and thereafter, at least once every three years, and make any amendments it determines are appropriate, having regard to the Policy's purposes, insights gained through the Service's deployment and experience with

BWCs, and academic or expert research findings concerning the use of BWCs by the Police Service.

JUNE 2021

**Appendix 'B' to Report
PSB 24-029**

**Model Governance Framework
for Police Body-worn Camera
Programs in Ontario**



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario



This guide by the Office of the Information and Privacy Commissioner of Ontario (IPC) is intended to enhance understanding of rights and obligations under Ontario’s access and privacy laws and advance best practices in relation to police use of body-worn cameras. It should not be relied upon as a substitute for the legislation itself or as legal advice. It does not bind the IPC’s Tribunal that may be called upon to independently investigate and decide upon an individual complaint or appeal based on the specific facts and unique circumstances of a given case. For the most up-to-date version of this guide, visit www.ipc.on.ca.

Contents

Background	1	Properly document the reasons for deactivation	11
Introduction	1	Limit the use of BWC recordings.....	12
Ensure lawful authority	3	Limit disclosure of BWC records to appropriate circumstances.....	13
Conduct a privacy impact assessment	3	Securely store, retain, and destroy BWC records	15
Scope out the BWC program	4	Respond to privacy breaches.....	16
Articulate guiding principles	4	Enforce compliance with policies and procedures.....	16
Define clear and appropriate purposes....	4	Conduct regular audits	16
Choose a vendor that supports compliance	5	Report annually on the BWC program	18
Conduct a pilot	7	Continually review and update the governance framework	19
Be transparent with the public	7	Appendix A	20
Train police officers before deployment...	8		
Establish rules for recording	8		

Background

In 2020, the Toronto Police Services Board and the Toronto Police Service engaged in extensive consultations with the Office of the Information and Privacy Commissioner of Ontario (IPC) regarding Toronto's body-worn camera (BWC) program and the related policy and procedures. The Toronto Police Services Board also held a public consultation with respect to the policy and procedures. Throughout this process, the IPC contributed by helping identify and define the key elements of a BWC governance framework necessary to meet the transparency and accountability expectations of Ontarians while also protecting their privacy and access rights. We commend the Toronto Police Services Board, and the Toronto Police Service, for their level of commitment and responsiveness demonstrated throughout the consultation. We were also fortunate to be able to coordinate our comments with those of the Ontario Human Rights Commission and were grateful to be able to take into consideration their important perspective as well.

Building on that practical experience and benefiting from what we learned through our in-depth engagement on the Toronto BWC program, the IPC developed this model BWC governance framework. We believe this governance framework can assist police services that are using or considering using BWCs do so in a manner that complies with Ontario's access and privacy laws and helps achieve consistency throughout the province. The framework can also assist police services boards in establishing the necessary checks and balances to carry out their important oversight role.¹

The IPC shared a draft of this governance framework with the Canadian Civil Liberties Association, the Ontario Association of Chiefs of Police, the Ontario Association of Police Services Boards, the Ontario Human Rights Commission, the Toronto Police Service, the Toronto Police Services Board, Christopher Parsons and Kate Robertson of the Citizen Lab, and Professor Alana Saulnier of Queen's University. The IPC appreciates the thoughtful comments provided by these organizations and individuals.

Introduction

BWCs are typically forward-facing cameras that are carried, fixed, or integrated on the uniform of a police officer and are capable of capturing both video and audio information as well as associated metadata.²

The IPC recognizes that there can be potential value in implementing BWC programs when properly governed. With the right parameters in place, such programs can create a documentary record of police-civilian encounters, including with respect to the use of force, and provide the public with accurate and timely information about those encounters. Receiving accurate and timely information is integral to transparency and being able to hold

¹ Where this framework refers to police service boards, it should be read as including requirements and best practices for both police services boards and the solicitor general who oversees the Ontario Provincial Police.

² Metadata is data about data. It describes and gives information about other data and can include date, time, location and duration of recorded activities. Metadata can allow for cross-referencing between datasets and be connected to identifiable individuals.

law enforcement officials accountable for their decisions and actions. Police use of BWCs may also have a positive impact on police performance and conduct.

In addition to their expectations of transparency and accountability, the public also holds dear their sense of privacy and expects it to be protected from the unwarranted gaze of the state. Accordingly, it is critical that a governance framework supports the implementation of a BWC program in a manner that respects individuals' reasonable expectation of privacy whether in private dwellings or in public places.³

This governance framework outlines the key transparency, accountability, privacy, and access considerations for the development of a BWC program. It is intended to help Ontario's police services and their boards comply with their obligations under Ontario's access and privacy laws, as well as provide best practices for BWC program implementation. It will also help Ontario's police services achieve consistency throughout the province.

This governance framework applies to the use of BWCs by law enforcement to capture video and audio in the course of their duties. It does not address the use of BWCs and any associated digital evidence management systems⁴ when they are equipped, integrated, or used in conjunction with live streaming capabilities, artificial intelligence or biometric technology (including facial recognition).

Augmenting BWCs with these, or any other sophisticated capabilities, is likely to raise additional privacy and security issues that require further analysis. As such, the IPC recommends that police services not adopt any such features until a full risk assessment is completed and the IPC is consulted. In addition, we recommend that police services generally refrain from using facial recognition technologies until lawful authority for doing so is clearly established, and their use is consistent with regulatory guidance issued by the federal, provincial and territorial information and privacy commissioners regarding the use of facial recognition by law enforcement.⁵

To assist with implementation of this governance framework, please see the checklist included as appendix A.

3 The Supreme Court of Canada has repeatedly recognized that members of the public have a reasonable, if diminished, expectation of privacy in public spaces. It follows that, if police are to deploy BWCs, the program must be designed and governed in a manner that is capable of accomplishing legitimate social objectives without incurring a disproportionate cost to fundamental rights and freedoms, including the right to privacy.

With respect to general privacy concerns, a **survey** prepared for the Office of the Privacy Commissioner of Canada indicates that the significant majority (92%) of Canadians expressed some level of concern about the protection of their privacy. Specifically, 37% are extremely concerned, 20% are concerned, and 35% are somewhat concerned.

4 A digital evidence management system is generally defined as a software application that allows for the secure uploading, storage and retrieval of digital files in various data formats. Several private sector vendors offer digital evidence management systems, including those using cloud-based platforms.

5 For a copy of the consultation draft of the federal, provincial and territorial facial recognition guidance, see **Notice of consultation and call for comments – Privacy guidance on facial recognition for police agencies**.

At this time the IPC is engaged with a number of police services regarding the governance of facial recognition in the context of mug shot databases, and expects to share key lessons as part of an effort to help ensure that the necessary safeguards and controls are in place to protect privacy and other fundamental rights.

Ensure lawful authority

Police services and their boards must identify their lawful authority for deploying BWC programs and ensure that their collection and use of BWC recordings align with that authority. They must also comply with the privacy and access to information rules set out in the *Freedom of Information and Protection of Privacy Act (FIPPA)* or the *Municipal Freedom of Information and Protection of Privacy Act (MFIPPA)* when they collect, retain, use or disclose personal information.⁶ In addition, as reflected in section 1 of the *Police Services Act*, police services must be provided in a manner that safeguards the fundamental rights guaranteed by the *Canadian Charter of Rights and Freedoms* and the *Ontario Human Rights Code*. Adherence to this Governance Framework does not necessarily imply compliance with the *Canadian Charter of Rights and Freedoms* or *Ontario Human Rights Code*.

Conduct a privacy impact assessment

When a police service plans to adopt BWCs or significantly change its BWC program or aspects of its overarching governance framework, the service is strongly encouraged to complete a privacy impact assessment (PIA). This also applies when a police service is contemplating a pilot BWC program. In addition, when novel or high-risk technologies are being contemplated, services are encouraged to consult the IPC.

FIPPA and *MFIPPA* do not require a PIA to be completed. However, PIAs are widely recognized as a best practice to assist institutions in complying with their privacy-related obligations. A thorough PIA will help to ensure that potential privacy risks are identified and that measures are taken to effectively mitigate these risks. Going through the systematic steps of a PIA will help ensure that the police service is able to identify its legislative authority to collect audio/visual recordings, and such collection aligns with the scope of their lawful authority and their related legal obligations, including obligations with respect to information security, records retention, access, use, and/or disclosure. Completing a PIA will also help ensure that the police service is able to justify its use of BWCs by showing that they are a necessary and proportionate response for addressing a real, substantial, and pressing social need.

The results of the PIA should be provided to the police services board to assist with its oversight role, and a summary of the PIA should be made publicly available for accountability and transparency reasons.

For more information on PIAs, refer to the IPC's publication, **Planning for Success: Privacy Impact Assessment Guide**.

⁶ Section 2(1) of *MFIPPA* and *FIPPA* define "personal information" as "recorded information about an identifiable individual," and includes a list of examples of personal information. Recorded information can be recorded in any format, such as paper records, electronic records, digital photographs and videos. A significant majority of images of individuals captured on BWCs are likely personal information as defined by Ontario's access and privacy laws.

Scope out the BWC program

BWCs should generally only be used to document officers' interactions with members of the public during the execution of their investigative and enforcement duties. In particular, they should only be used to capture specific investigative or enforcement incidents that involve direct encounters or engagements with members of the public. BWCs must not be deployed to record all the time, including as a tool of mass or generalized surveillance. Nor should they be used to surreptitiously record individuals.

Articulate guiding principles

Police services boards should anchor their BWC policies in a statement of overarching guiding principles. These principles should be developed and implemented to support a program that respects privacy and other fundamental human rights, including those guaranteed by the charter and the *Ontario Human Rights Code*.

A BWC governance framework should include a statement of principles that addresses the provision of fair, effective, and equitable policing services. At minimum, such a statement of principles should commit to using BWCs in a manner that:

- is necessary and proportionate to the purposes of the program, clearly defined
- is transparent and accountable to the public
- upholds the integrity of the criminal justice system and the administration of justice
- protects individuals' rights to information and privacy
- treats everyone fairly and equitably
- respects the inherent worth and dignity of human beings

Define clear and appropriate purposes

When developing policies and procedures, boards and police services should clearly state the purposes of their BWC program. Purposes for deploying BWCs include:

- enhancing transparency and police accountability
- ensuring that audio-visual recordings of investigative and enforcement interactions with the public are accurately and systematically captured and stored
- enhancing public and police officer safety, including by reducing use of force incidents
- providing evidence for investigative, judicial and oversight purposes
- ensuring fair and timely response to allegations of police misconduct and resolution of complaints
- supporting the goal of achieving bias-free policing
- enhancing training and improving police policies and procedures
- enhancing public trust and confidence in police

Choose a vendor that supports compliance

Police services and their boards must ensure that their BWC vendor is able to implement the service's legal requirements. All applicable contracts between them must contain terms and conditions that support compliance with Ontario laws (including restrictions on access and use for secondary purposes). Among other things, this means that the prospective vendor must be able to configure the equipment in a manner that ensures a robust audit trail and can satisfy transparency, accountability, access and privacy obligations, including security safeguards.

Police services should consult closely with technical advisors, privacy professionals, and legal counsel in their vendor procurement and selection processes.

The following is a non-exhaustive list of transparency, accountability, access and privacy related factors that a police service should consider when purchasing BWC equipment:

Video and audio quality

Police services need to determine the appropriate video resolution and audio quality being captured by the BWCs. The video and the audio of some cameras can substantially outperform what the human eye and ear can perceive. For instance, the resolution and field of view of a camera can be far greater than that which is necessary or proportionate to the public safety aims of the BWC program. As a result, the camera may record identifiable images of individuals who had no involvement in a police-civilian interaction and who were never notified that they were being recorded, including those in the far background. For privacy and other reasons,⁷ it may be appropriate to consider procuring cameras that have video and audio capabilities more in line with the limits of human eyesight and hearing. Also, vendors should be able to offer redaction features such as blurring and audio distortion capabilities in order to protect the privacy of, for example, passers-by or other individuals who are inadvertently captured in the field of view.

Visibility of the camera and its use

Size, mounting, and other features of the cameras can affect their visibility and transparency to the public. For instance, the size of the BWC can make it more or less conspicuous to individuals in the immediate vicinity of the officer.

There are also several mounting positions available for BWCs. For instance, many police services choose chest mounted BWCs. Other options include mounting the camera on an officer's arm, helmet or glasses. Whichever mounting option is used, it is important to ensure that the cameras are sufficiently apparent to individuals around them to provide for transparency and openness.

Some devices have a forward facing display, which increases their visibility and allows those being recorded to see their image in real time, while others have a light and audio signal to indicate that the camera is on.

⁷ It may also have implications for when the recordings are reviewed, as it may be assumed that the officer's perception matches that of what is captured on the BWC.

BWCs may also come equipped with a stealth mode, also known as covert mode. This feature allows the BWC to record without providing visual or audible notice that it is recording. Stealth mode should only be used in rare situations where activating the camera in its normal mode is likely to endanger officer safety.

Pre-event recording

Most BWCs continuously record throughout the period they are powered on, but the footage being captured is automatically overwritten at certain set intervals (e.g., every 30, 60, 90, or 120 seconds). Once the cameras are fully activated however, this overwriting process stops. At that point, all video and audio elements are recorded and preserved. This includes the period of time immediately prior to activation that coincides with the same interval of time at which the camera's overwriting process has been set. Known as pre-event recording, this recording function helps to capture the initial stages of an investigative or enforcement incident involving a member of the public.

To provide the necessary context and help enhance perspective and understanding of a given situation, a BWC's pre-event recording time should be configured to sufficiently capture the critical moments leading up to direct encounters or engagements with members of the public. To provide further context, BWCs should also have the capacity to record the exact date, time, and location of when and where they begin recording.

Activation of cameras

The user can activate most BWC recording functions manually. However, other activation options based on automated sensors are available in some camera systems. For instance, sensors placed in a police vehicle's light bar/siren or an officer's holster can automatically activate the camera's audio and video recording functions when lights or sirens are turned on or when an officer's weapon is drawn. These features should be carefully considered and employed to ensure that BWCs are sufficiently sensitive and responsive (but not overly so).

BWCs generally come with the capacity to record the exact date, time, and location of when and where they begin recording.

Auditing

When a police service and its board consider using third party service providers for elements of its BWC program, it must ensure the vendor's system has the necessary auditing capabilities.

The vendor must be able to ensure that all actions, including recording, indexing, accessing, viewing, copying, modifying, redacting, and destroying data in the BWC system can be logged and auditable. The audit trail should include the login details used to access the system such as the username and point of access, as well as date, time, and duration of access.

Auditing capacities and requirements must be clearly defined in all the appropriate service agreements with the vendor.

Conduct a pilot

Police services should adopt an incremental approach to implementing a BWC program. The IPC recommends that police begin by planning and conducting a pilot (also called a test phase) prior to full scale implementation. The pilot is also an opportunity for the police service to experiment with different BWC vendors and to see how officers respond to the technology.

When planning to conduct a pilot, a police service and its board should address the following matters:

- consult with community members, particularly those likely to be impacted by a BWC program, and seek input from appropriate stakeholders, including civil society groups
- define the purposes, goals, objectives, and scope of the pilot
- establish what will be measured during the pilot (e.g., proper activation and deactivation of BWCs, impact of cameras on conduct and behaviour, reduced use of force incidents)
- establish the appropriate administrative supports for data collection and analysis that will guide the pilot and its evaluation

There should be an evaluation process at the conclusion of the pilot that includes further public engagement. A report describing the pilot and its evaluation should be prepared and the report, or a summary of it, should be made publicly available. If a decision is made to proceed with a BWC program, the report will assist in making any necessary adjustments and confirming the final elements of the program, including a clear governance framework.

Be transparent with the public

Police services should develop and implement appropriate notices that are sufficiently transparent to inform the public of the deployment of BWCs.⁸

Verbal notice: Police officers should inform members of the public that they are being recorded at the earliest opportunity during any interaction that involves use of BWCs. Police should also inform other officers and first responders that they are being recorded using a BWC.

Visual and auditory notice: Police officers should wear their BWCs in plain view with a sticker, emblem or some other form of visual notification indicating that they are wearing a recording device. Where the selected BWC has such a capacity, police should activate and maintain the light and audio signal to indicate that the camera is on unless doing so would likely endanger officer safety.

⁸ **Section 39** of *FIPPA* and **section 29** of *MFIPPA* provide that, as a general rule, an individual must be informed of: (a) the legal authority for the collection; (b) the principal purpose or purposes for which the personal information is intended to be used; and (c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

Written notice: Additional notice should also be provided to the public, including through information published prominently on the police services board and police service’s website and social media platforms to inform the community of the BWC program.

Requirements should also be in place to ensure that up-to-date information is posted on the police services board and police service’s website concerning the collection of BWC recordings, including:

- the most current version of the board’s BWC policies and the service’s BWC procedures
- a description of what information is being collected by BWCs and for what purposes
- the applicable retention periods
- how individuals can complain about the use or lack of use of BWCs
- how individuals can make requests to view, access or seek the public release of such recordings
- information about how to appeal to the IPC where an access to information request is denied in whole or in part, and
- a copy of the police service’s most recent annual report to its board (for more information, see section on annual reports in this document)

Train police officers before deployment

Police services should establish training requirements for all officers to fulfill prior to being issued a BWC. Subsequent refresher training on an annual basis should also be required. The goal of the training is to ensure the continued effective and lawful use and operation of the BWC. Training topics to be addressed include: understanding the purposes, goals, and objectives of the BWC program; providing notice and being transparent about the use of BWCs, activation and deactivation requirements; the uploading and securing of BWC recordings and metadata; access controls and use and disclosure limitations. Case studies could serve as an effective means of contextualizing training. For instance, through concrete examples, officers can enhance their understanding of the different scenarios in which the police service rules permit them to limit a BWC’s recording capacity depending on the relevance, urgency, and sensitivity of a given situation.

Training programs should be reviewed regularly to ensure they continue to reflect best practices (including those obtained from practical experience) and incorporate changes, updates, or other revisions to policy, procedures, and equipment.

Establish rules for recording

Recording requirements for the use of BWCs should be governed by clearly defined policies and procedures. Changes to a police services board’s policies or a police

service's procedures should be limited and made only with sufficient justification and appropriate approvals.

To help ensure that a BWC program can accomplish its purposes, including those that relate to transparency and accountability, BWC recordings should generally be mandatory for the full duration of any calls for service and all other investigative or enforcement-type engagements that involve a police officer and a member of the public. This approach to recording should be followed from the very beginning to the very end of the police-civilian contact.

The requirement to record the full encounter should only be subject to a limited and exhaustive list of necessary exceptions. In particular, any mandated or discretionary exceptions to the duty to record should be restricted to those that can be justified and clearly defined within explicit and limited circumstances.

When to record

Officers should be required to activate the BWC prior to interacting with any member of the public in relation to a call for service. In addition, when interacting with a member of the public outside of a call for service, all attending officers should be required to activate their BWCs as soon as it is determined that the engagement is for a law enforcement or investigative purpose. Such interactions will include apprehensions under the ***Mental Health Act***, interactions with persons in crisis and regulated interactions or street checks.

As such, individuals will generally not have a right to refuse to consent to being recorded by police when police are actively conducting an investigation or enforcing the law (e.g., in a public place). In this context, police policies and procedures should provide that if a member of the public requests that an officer stop recording or refrain from recording in circumstances where the officer is required or permitted to record and the individual is not being detained or under arrest, the officer must:

- (i) inform the individual that while the camera must stay on, they are free to discontinue the interaction, including by leaving the scene
- (ii) respect their right to do so⁹

To help ensure that a full picture of the initial stages of police encounters with the public are captured, the BWC governance framework should require a BWC's pre-event recording capacity to record both audio and video for a minimum period of 30 seconds, if not longer. The precise period (e.g., 30, 60, 90, or 120 seconds) should be determined as a function of the intended purpose, that is, to provide sufficient context leading up to an investigative or enforcement related police-civilian encounter, while taking into consideration the privacy interests of police officers with respect to their incidental personal conversations. The BWC governance framework should also ensure that the date, time, and location of BWC activation and deactivation are recorded.

⁹ With respect to the right to discontinue such an interaction, see, for example, the discussion of psychological detention and the freedom to leave in *R. v. Grant*, 2009 SCC 32 (CanLII), *R. v. Suberu*, 2009 SCC 33 (CanLII), and *R. v. Le*, 2019 SCC 34 (CanLII) and *O. Reg. 58/16* (Collection of Identifying Information in Certain Circumstances - Prohibition and Duties). Also see the Toronto Police Services Board's Policy on **Regulated Interaction with the Community and the Collection of Identifying Information** and the Toronto Police Service's **KnowOur Rights** webpages.

When not to record

To respect privacy and other fundamental rights, officers should be directed not to record:

- during policing-civilian contact or activities that are not investigative or enforcement in nature (e.g., informal interactions)
- while attending in a courthouse, except in exigent circumstances, or under legal authority
- during strip searches or body cavity searches

Recording rules for special and sensitive settings

Recording in a healthcare setting: Officers should be directed not to record in healthcare settings, except:

- in exigent circumstances
- under the authority of prior judicial authorization
- where the officer has custody of a person who is waiting for health care treatment and the officer is alone with that person
- where the officer has custody of a person who is being treated or is waiting for health care treatment and the officer reasonably believes that the interaction between the officer and the person in his or her custody requires or might soon require the use of force, or
- with the express consent of any persons who might reasonably be expected to be captured in the recording

Recording in a private dwelling: Officers should only be permitted to record in private dwellings, such as residences, where:

- there are exigent circumstances
- under the legal authority of a warrant, or
- in a situation where an officer's lawful presence in a private place is conditional on the owner's/occupant's consent to being recorded, and the officer has provided the owner/occupant with a reasonable opportunity to refuse such consent. If the owner/occupant requests that the interaction not be recorded, the officer must stop recording

Recording in religious and spiritual places: Given the heightened privacy-related sensitivities associated with many religious or spiritual settings, policies and procedures should expressly remind police officers not to record except in relation to a specific investigative or enforcement purpose. In addition, to minimize intrusion, an officer should provide individuals present — including any Elders, Knowledge Keepers, or other leaders — a clear explanation of the reasons that BWC recording is necessary.

Recording at a protest: BWCs must not be used to carry out general surveillance or to dissuade members of the public from exercising their fundamental rights to assemble, demonstrate or protest peacefully. By default, BWCs should be deactivated when police

officers are attending such events or occurrences. On these occasions, BWCs should only be activated:

- when an officer engages, or is about to engage, a member of the public to investigate a breach of the law
- when an officer attempts to enforce the law, or
- if an infraction of the law is occurring or the officer reasonably believes that a significant infraction of the law is imminent

Limited discretion to deactivate recording

Rules should also be established to limit officers' discretion to deactivate the BWC recording function, or obstruct or reduce the BWC recording capacity during an investigative or enforcement occurrence involving a member of the public. Discretion to deactivate or otherwise limit the recording should only be permitted if it can be justified and properly defined in a police service's rules.

A rule should be established to address situations where it may be necessary to momentarily obstruct, re-orient or deactivate the BWC video or audio to minimize intrusions on a person's dignity or vulnerability during a police officer engagement. For instance, a rule should be provided to allow police to deactivate the video function of a BWC for a sufficient period of time to allow a person time to cover up when they are in a state of undress, including while using a toilet. Police may also consider establishing a rule permitting officers to momentarily obstruct or re-orient a BWC's video function to the extent necessary to reduce the risk of aggravating emotional harm or trauma to a victim of sexual assault or domestic violence.

In all cases, the rules should make it clear that BWC capacity deactivation/limitations should be restricted to only those necessary to address the overriding concern. The rules should specify the length of time of the limitation and whether the limitation applies to video and/or audio. Rules permitting officers to deactivate both video and audio recording will be particularly difficult to justify.

Properly document the reasons for deactivation

Comprehensive record keeping requirements should be established to require the documentation of all intentional and accidental deactivations and limitations of a BWC's recording functions. In the event that the BWC recording accidentally or unintentionally stops, the officer should restart the recording at the earliest opportunity and note the reason the recording was stopped on video and in their memorandum book. In the event that an officer has decided to deactivate or limit the BWC's recording capabilities or is directed to do so by their supervisor, the officer should record a brief audible statement indicating the reason why the BWC is being deactivated or its recording functions otherwise limited. Where a supervisor directs the deactivation or limitation, the supervisor should also document the deactivation or limitation-related direction.

Limit the use of BWC recordings

Personal information collected by BWCs should only be used for the purpose for which it was collected or for a consistent purpose.¹⁰ The use of the information for secondary purposes is generally not permitted under Ontario’s access and privacy laws and should be strictly limited. For instance, BWC recordings and any related data — hereafter records — must not be mined to feed intelligence gathering or accessed without lawful justification (e.g., as part of a fishing expedition).¹¹ In addition, BWC records must not be accessed for personal reasons or for the purpose of causing harm or embarrassment to persons. Nor should BWC systems or BWC records be used to facilitate mass surveillance of the general public.

The BWC governance framework should include rules that set explicit limits with respect to the use of BWC records, as supported by detailed role-based access controls. Authorized persons should only be permitted to access BWC records if their duties and functions justify and necessitate such access, and the right to access and use BWC records has been clearly identified in a policy or procedure. Additionally, any person who has access to BWC records may not provide access to those records to other police service staff or any other individual without lawful authority. All accesses to BWC records should be logged and fully auditable. This includes the identity of the person accessing the information, the date and time of the access, and the reason for the access.

The circumstances where BWC records may be accessed and used by appropriate staff include the following:

- review by the officer who wore the BWC which captured the recording after the officer has completed any required initial notes, reports, statements and interviews regarding the recorded events
- to allow officers’ supervisors to fulfill their duties, including those related to the regular periodic review of BWC records, to: (i) identify and address potential bias and discrimination; (ii) address specific allegations of misconduct; and (iii) oversee and address any concerns associated with the use of force
- for the purpose of review by forensic identification service staff responsible for analysis in relation to specific BWC records
- to allow law enforcement personnel to conduct a criminal or quasi-criminal investigation when there are grounds to believe the records include evidentiary materials relevant to that investigation¹²
- by designated persons for the purpose of conducting a sexual violence case review

10 **Section 41(1)** of *FIPPA* and **section 31(1)** of *MFIPPA* restrict how personal information may be used once it has been lawfully collected. As a general rule, the acts prohibit the use of personal information unless the institution obtains consent from the individual to whom the information relates or the personal information is used for the purpose for which it was obtained or compiled or for a consistent purpose. A “consistent purpose” is defined in **section 43** of *FIPPA* and **section 33** of *MFIPPA* as a use of personal information that the individual to whom the information relates might reasonably have expected at the time of collection.

11 In *Imperial Manufacturing Group Inc v Decor Grates Incorporated*, **2015 FCA 100**, at **para 38**, the Federal Court of Appeal characterized a fishing expedition as “a search by an empty-handed party looking for something to grasp onto.”

12 Persons accessing BWC records may include members of other police services or other criminal or quasi-criminal authorities who are conducting an investigation as agents for the service that generated the BWC records.

- to allow a police officer, a police service's legal counsel, or staff members supporting them to assess and prepare evidence for use in an on-going or potential criminal or civil proceeding
- to enable internal reviews or investigations, such as professional standards, or external criminal or conduct investigations
- for the purpose of conducting a review or audit required of or by the police service or its board
- for purposes directly related to a possible compelling public interest release

Police services must ensure that sufficient access controls and related safeguards are in place to protect the privacy of complainants and witnesses who are minors and all those dealt with under the *Youth Criminal Justice Act*, including those who are merely cautioned or warned under that act.

Police services should restrict the use of personal information in BWC records for training purposes when other less privacy invasive alternatives are available. If a BWC recording is determined to have value for training purposes and appropriate approval for such use is obtained, anonymizing measures should be taken to the greatest extent possible to conceal the identity and protect the dignity of the individuals in the recording. This may include blurring¹³ and voice distortion.

Limit disclosure of BWC records to appropriate circumstances

FIPPA and *MFIPPA* prohibit the disclosure of personal information, except in the circumstances identified in **sections 42(1) and 43** of *FIPPA* and **32 and 33** of *MFIPPA*. Police services and their boards should develop policies and procedures to ensure that any disclosures of BWC records are consistent with these sections.

Facilitate access to BWC records as appropriate

Individuals whose personal information is held by Ontario police have a right of access to that personal information under **section 47(1)** of *FIPPA* and **section 36(1)** of *MFIPPA*.¹⁴ Members of the general public, civil society groups, journalists, etc. also have a general right of access to information under **section 10** of *FIPPA* and **section 4** of *MFIPPA*.¹⁵ Accordingly, processes must be in place to respond to requests and enable individuals or their representatives to exercise their legal right to access BWC records, including in cases that capture an incident in which they themselves were involved.

In addition, police services and their boards are encouraged to establish a process by which members of the public or their representatives may be allowed to view BWC recordings capturing an incident in which they were involved. This review may be used for the purpose

¹³ This should not be limited to faces but to any information that could be used to identify an individual (e.g., tattoos).

¹⁴ Subject to the statutory exclusions and exemptions.

¹⁵ Subject to the statutory exclusions and exemptions.

of attempting to informally resolve a complaint or a potential complaint related to a policy matter, service issue or conduct of one of its officers.¹⁶ The process should facilitate timely review so that an individual may view a recording and still have sufficient time to decide whether to pursue a formal complaint.

Where a recording captures personal information of individuals who do not consent to its viewing or release, the service must have the capability to sever the recording by, for example, blurring out the images or distorting the voice of these non-consenting individuals prior to making the recording available. The recording should be anonymized, but only to the extent necessary to protect the privacy of these other individuals or to protect necessary confidentiality. For instance, it may be necessary to sever information, which if disclosed, could reasonably be expected to interfere with a law enforcement matter, endanger the life or physical safety of any person, or deprive a person of the right to a fair trial.

In cases where the police refuse a request for access to, or viewing of, BWC records, the reason for the refusal must be provided to the requester in writing and the individual must be informed of their right to file a complaint, or appeal the decision to the IPC. For more information about filing an **appeal** or a **privacy complaint** visit www.ipc.on.ca.

Consider disclosing BWC records in the public interest

Policies and procedures should provide for public interest-based disclosure of BWC records in special circumstances to address compelling concerns about, for example, human rights and police use of force, as well as allegations of discreditable conduct, improper conduct, or misconduct. A public-interest based disclosure may be made proactively by the police service or in response to a formal access to information request as discussed above.

In deciding whether to release BWC records in the public interest, all relevant factors should be considered by a senior officer including:

- what is consistent with the law
- what is reasonable in the circumstances of the case
- whether withholding a recording or a portion of a recording is necessary to protect the integrity of an ongoing investigation or a pending judicial or quasi-judicial proceeding
- whether withholding a recording or a portion of a recording from the public is likely to undermine public confidence in policing or the administration of justice

Note that while a police service may be precluded from disclosing a BWC record during an ongoing investigation by the Special Investigations Unit (SIU) or the Office of the Independent Police Review Director of Ontario (OIPRD), this limit to access will generally lapse once the SIU or OIPRD role has concluded.

If a decision is made to release BWC records in the public interest, measures should be employed to protect necessary confidentiality and to obscure any information that could be used to identify an individual. This may include blurring and voice distortion, unless the service is required by law to release the recording in another form or the affected individuals

¹⁶ The option to request an opportunity to view a recording is separate from and additional to the statutory right to request access to and receipt of a copy of a record.

have consented to the release of their personal information. With the exception of these privacy protective measures, when a decision is made to release in the public interest, the full and unedited copy of the recording should be released and accompanied by an explanation justifying the public interest release decision.

In the event a request for the compelling public interest release of a BWC record is denied in whole or part, written reasons should be provided by the senior officer explaining why the record or a portion of the record cannot be released. It should also inform them of their right to file a complaint or appeal with the IPC.

Cooperate with relevant oversight bodies

A comprehensive governance framework must include provisions that ensure the timely disclosure of all relevant BWC records to the bodies responsible for independent oversight of police (e.g., the OIPRD and the SIU), when required.

Securely store, retain, and destroy BWC records

Appropriate measures must be taken to secure BWC records.¹⁷ As previously mentioned, BWC records include both the recordings as well as any meta-data produced by the BWC and other related data. BWC records must be encrypted on the BWC device, during transit, and while in storage. In light of the sensitive nature of the information collected by BWCs, BWC records should be stored and processed on storage servers located in Canada.

Police services and their boards should establish clear and proportionate retention periods for BWC records. Retention periods must be sufficiently long to facilitate the right of access and related rights to file complaints or civil suits, and sufficiently short so that BWC records are not retained longer than is reasonably required for a valid purpose. For instance, in order to ensure BWC records are preserved long enough to account for timelines for commencing a civil suit, BWC records should be retained for a minimum period of 30 months plus one day.¹⁸ Immediately thereafter, BWC records should be securely destroyed unless a relevant and appropriate circumstance arises that triggers a longer retention period. A system should be in place to ensure that BWC records are marked for retention as soon as a complaint, investigation, legal action or other relevant and appropriate triggering event is filed or initiated.

Police services and their boards should also have clear rules requiring the secure destruction of BWC records at the expiration of the applicable retention period, with technical measures in place to ensure that the information is securely destroyed in a timely fashion.

¹⁷ Section 4 of **Regulation 460** of *FIPPA* and section 3 of **Regulation 823** of *MFIPPA* require institutions to protect personal information in their custody or under their control from unauthorized access and inadvertent destruction or damage.

¹⁸ This retention period ensures the records are retained for the duration of the general two-year limitation period established by the *Limitations Act, 2002* and the six month-period a plaintiff is permitted to serve a defendant after filing a lawsuit with a court under Rule 14:08 of *Ontario's Rules of Civil Procedure*.

Respond to privacy breaches

Police services and their boards should establish rules on how they must respond to potential or actual instances of unauthorized access or disclosure of personal information (i.e., privacy breaches). These rules should include breach containment, mitigation, and notification requirements. Contracts with third party service providers must address their obligations with respect to responding to a breach. Those responsibilities include promptly notifying the police about any potential or actual breach, as well as providing relevant information to, and otherwise cooperating with, the police to facilitate timely investigation into the breach.

Police services should notify the IPC as soon as reasonably possible in the event of any significant privacy breaches. In assessing whether a privacy breach is significant, police services should consider all the relevant circumstances, including whether:

- the personal information at issue is sensitive, either by its nature or given its context
- the breach is likely to cause significant harm, including financial, reputational, or emotional harm, such as embarrassment or humiliation
- the breach involves the personal information of a large number of individuals
- the likelihood that the personal information at issue could be misused, or further disseminated by others; or
- the police service is having difficulties containing the breach

For more information on how to respond to a privacy breach, refer to the IPC's publication, **Privacy Breaches Guidelines for Public Sector Organizations**.

Enforce compliance with policies and procedures

Compliance with policies and procedures must be enforced. Police services should establish clear disciplinary measures for officers who willfully fail to comply with BWC policies and procedures. For instance, an officer may face mandatory minimum sanctions in the event it is determined they have intentionally failed to activate a camera in circumstances where activation is required or intentionally deactivated the camera prematurely. It may be appropriate that officers are given a limited grace period (for instance, 60 days) to familiarize themselves with the BWC policy and procedures before formal sanctions are applied.

Conduct regular audits

A robust audit regime will contribute to accountable and transparent policing, as well as help protect BWC records from unauthorized access, modification, and destruction and ensure the integrity and continuity of evidence.

In addition to being used to identify and address any potential non-compliance issues, auditing should also be used to identify good policing, highlight examples of exemplary performance, and improve best practices. Audit findings should inform the evolution of best practices and any necessary changes to BWC policies and procedures.

Audits should be governed by clearly defined policies and procedures.

Police services and their boards should establish rules to ensure that all actions, including recording, indexing, accessing, viewing, copying, modifying, redacting, and destroying data in the BWC system are logged and auditable. The audit trail should include the login details used to access the system such as the username and point of access, as well as date, time, and duration of access.

With respect to compliance reviews, police services should require scheduled (e.g., monthly and annual) and event-based audits of BWC records to assess compliance with all applicable laws, policies, procedures and professional standards, including those related to discrimination and the use of force.

Board policies and service procedures should set out how supervisors will select BWC records for review. This review process should be clearly defined, fair and defensible. In this context, police services and their boards should consider conducting scheduled audits based on a random sample of certain matters including:

- incidents where a complaint was filed under the *Police Services Act*, *FIPPA*, *MFIPPA*, the *Ontario Human Rights Code*, or a civil suit under the *Courts of Justice Act*
- incidents where there was a use of force
- incidents of data breach
- incidents that resulted in detention or arrest
- incidents that were initiated by a call for service
- incidents that were not initiated by a call for service
- incidents where a BWC was intentionally or accidentally deactivated or had its recording functions limited, prior to the end of an investigative or enforcement incident
- incidents whose retention period expired during the reporting period

Reviewers of the BWC records should assess whether:

- activation and deactivation of the recording are in compliance with police policy and procedure
- the subject of the recording is informed at the earliest opportunity in the interaction that the interaction is being recorded for video and audio
- in applicable circumstances, the officer: (i) informs the individual(s) that while the camera must stay on, they are free to discontinue the interaction, including by leaving the scene; and (ii) respects their right to discontinue the interaction
- any limitation of the recording function of the BWC is justified and of reasonable duration
- all access to the BWC records is justified and necessary

- all requests for BWC records from the SIU or the OIPRD are fulfilled in a full and timely manner
- the service is in compliance with required retention and destruction practices

In conducting scheduled audits, reviewers should also:

- identify and initiate steps to address evidence of bias and discrimination
- identify and initiate steps to address the need for additional training or other measures
- identify good policing and examples of exemplary performance, including for the purposes of enhancing training, improving police policies and procedures, and achieving effective, bias-free policing

Audit processes and results should be documented and include analyses, findings, and any recommendations for improvement.

Report annually on the BWC program

Police services boards should establish rules requiring the production of annual public reports from their respective police service regarding compliance with key laws, policies and procedures, and periodically lead evidence-based evaluations of the BWC program, policies, and procedures. Annual reports should also include details of the various audits conducted throughout the reporting year.

Police services boards should consider requiring that each annual public report include:

- analysis, findings, and recommendations of the annual audit (or a summary)
- the number of complaints received by the police service with regards to the use or failure to use BWCs, a summary of the complaints, and a summary of the dispositions of the complaints during the reporting period
- the total number of *Police Services Act*, *FIPPA*, *MFIPPA*, and the *Ontario Human Rights Code and Police Services Act* complaints and civil suits received by the police against its staff, and the number of such matters for which there was a relevant BWC recording, broken down by proceeding and resolution status
- the total number of use of force incidents and the total number of such incidents captured by BWC footage
- the total number of BWC recordings currently stored by the police service beyond the default retention period, broken down by the reason for the extended retention period, as well as the total number of incidents of premature destruction of BWC records
- the number of reports submitted documenting the reason for not activating a BWC prior to the beginning of an interaction with a member of the public or not recording through to the end of such interaction, and the number of these incidents, if any, found to not be in compliance with the BWC policy or procedure
- the number, if any, of BWC records requested by the SIU or the OIPRD, which were not fulfilled within 30 days and a summary of the reasons for delay

- the total number of BWC records released as part of a disclosure process in a legal proceeding
- the number of police service staff disciplined for lack of compliance with the BWC policy or procedure and a summary of the disciplinary measures used
- the number of requests for the identification of individuals in images from BWC recordings using the police service's mug shot database, and the percentage of such requests out of the total number of requests for use of the database
- the number of investigations of potential privacy breaches during the reporting period, the number of such incidents determined to constitute a breach and a summary description of these incidents, the number of times the IPC was notified of a significant breach, and the number of affected individuals who were notified of a breach
- the number of requests made by members of the public to view, access or seek release of BWC records, the number of requests that were refused, if any, and a summary of the reasons for any refusals
- the number of BWC records disclosed at the initiative of the police in the public interest, and reasons for the disclosure
- a review of whether the deployment of BWCs is achieving its prescribed purposes, whether their use remains justified in light of these purposes, and whether their use has resulted in any unintended negative impacts, including, but not limited to:
 - use of force trends over the past five years
 - complaint trends over the past five years
 - findings from a survey of public trust in the Service
 - findings from consultations with impacted and marginalized communities.

Continually review and update the governance framework

Police services and their boards should review their BWC policies and procedures periodically to ensure that they continue to align with the service's BWC program guiding principles and purposes. Additionally, new insights may be gained from data collected and analysed by the police service in the course of its BWC deployment, audit and review findings, and/or as new academic or expert research findings come to light, which could require changes to the policies and procedures. The periodic reviews should include opportunities for further consultations and engagement with relevant stakeholders and members of the public.

Appendix A

Checklist: Implementing a body-worn camera (BWC) program



Ensure lawful authority

- Identify lawful authority to deploy the BWC program
- Ensure the collection and use of BWC records align with that lawful authority

Conduct a privacy impact assessment (PIA)



- When planning to adopt or significantly change a BWC program (including a pilot), conduct a PIA
- Review the IPC's **Planning for Success: Privacy Impact Assessment Guide** against your own PIA policies and procedures
- Identify and consult with internal and external stakeholders, as well as key subject matter experts
- Make changes to the program, policies and procedures and any other recommended changes as a result of the PIA
- Provide the results of the PIA to the police services board
- Publish the PIA or make a summary of the PIA publicly available
- Review and update the PIA as necessary over time, and adapt the program, policies, and procedures accordingly



Scope out the BWC program

- Define the scope of the BWC program
- Use BWCs only to capture specific investigative or enforcement incidents involving direct encounters between police officers and members of the public
- Do not use BWCs to record all the time
- Do not use BWCs to surreptitiously record individuals
- Do not use BWCs as tools of mass or generalized surveillance

Articulate guiding principles



- Draft a statement of guiding principles that support respect for the right to privacy, access to information, and other fundamental human rights
- At minimum, these principles should commit to using BWCs in a manner that:
 - is necessary and proportionate to the purposes of the program, clearly defined
 - is transparent and accountable to the public
 - upholds the integrity of the criminal justice system and the administration of justice
 - protects individuals' rights to information and privacy
 - treats everyone fairly and equitably
 - respects the inherent worth and dignity of human beings



Define clear and appropriate purposes

- Clearly define and state the purposes of the BWC program
- Ensure those purposes are appropriate and within the scope of the program

Choose a vendor that supports compliance



- Ensure the BWC vendor is able to implement the service's legal requirements
- Define desired equipment specifications and features to satisfy transparency, accountability, access and privacy obligations – including robust security safeguards and auditing capabilities
- Consult with technical advisors, privacy professionals and legal counsel
- Ensure vendor contracts support compliance with Ontario's laws



Conduct a pilot

- Plan and conduct a pilot prior to full scale implementation of BWCs
- Consult with community members likely to be impacted by the BWC program
- Define the purposes, goals, objectives and scope of the pilot
- Identify what will be measured during the pilot
- Establish appropriate administrative supports for data collection and analyses during the pilot
- Conduct an evaluation and assess the findings at the end of the pilot
- Publish the evaluation report, or a summary, describing the pilot and the evaluation results

Be transparent with the public



- Develop and implement appropriate notices that are sufficiently transparent to inform the public of the use of BWCs (including verbal, visual and auditory, and written notices)

- Publicly post up-to-date information concerning the collection of BWC records on the boards' and services' websites



Train police officers before deployment

- Establish training requirements that officers must fulfil prior to being given BWC equipment
- Provide refresher training on an annual basis
- Regularly review the training program to ensure that it continues to reflect best practices
- Incorporate changes, updates, and other revisions as necessary, resulting from PIAs or audit report findings

Establish rules for recording

REC

- Establish clear rules for when to record and when not to record
- Require mandatory recording (including pre-event recording) throughout the full duration of any investigative or enforcement related encounter between police officers and members of the public
- Limit any mandatory or discretionary exceptions to only those that can be justified and clearly defined within explicit and limited circumstances
- Establish clear restrictions on officers' discretion to deactivate BWC recording functions or momentarily obstruct or reduce recording capacity in particularly sensitive situations
- Establish clear rules for recording in special settings, including in healthcare settings, private dwellings, religious or spiritual places, or at public protests



Properly document the reasons for deactivation

- Establish comprehensive record-keeping requirements to ensure that police officers properly document all intentional and accidental deactivations and limitations of BWC recording functions. This includes supervisors who directed the deactivation or limitation.

Limit the use of BWC recordings



- Establish rules that set explicit limits with respect to the use of BWC records
- Clearly identify and define who has access to BWC records and for what purpose.
- Ensure that all accesses to BWC records are logged and fully auditable
- Ensure that sufficient access controls and related safeguards are in place to protect the privacy of complainants and witnesses who are minors and all those dealt with under the *Youth Criminal Justice Act*



Limit disclosure of BWC records to appropriate circumstances

- Limit disclosure of BWC records to only those permitted by law
- Develop policies and procedures for responding to access requests for BWC records
- Develop processes to allow members of the public to view BWC recordings
- Develop policies and procedures that address disclosure in the public interest
- Develop policies and procedures that address timely disclosure to police oversight bodies

Securely store, retain, and destroy BWC records



- Ensure BWC records are encrypted on the BWC device, during transit and while in storage
- Establish clear and proportionate retention periods for BWC records that are sufficiently long to facilitate right of access, and sufficiently short so as not to retain records longer than reasonably required
- Establish clear rules for the secure and timely destruction of BWC records at the end of the applicable retention period



Respond to privacy breaches

- Develop a protocol for immediately responding to privacy breaches and escalating matters as appropriate
- Include breach containment, mitigation, and notification requirements
- Ensure third party contracts address vendors' obligations to respond to privacy breaches as well
- Take necessary steps to prevent future privacy breaches through remedial measures, training and education
- See IPC's **Privacy Breaches: Guidelines for Public Sector Organizations**

Enforce compliance with BWC policies and procedures



- Enforce compliance with BWC policies and procedures
- Establish and communicate clear disciplinary measures that will be taken in the event of non-compliance
- Impose disciplinary measures in cases of non-compliance, as applicable



Conduct regular audits

- Establish clearly defined policies and procedures to govern the audits
- Ensure that all activities in the BWC system are logged as part of a robust audit trail
- Conduct regularly scheduled and event-based audits to ensure compliance with BWC policies and procedures
- Document audit processes and results, including analyses, findings, and recommendations
- Use audit findings and recommendations to inform the evolution of best practices and any necessary changes to BWC policies and procedures

Report annually on the BWC program



- Establish clear rules requiring the production of annual public reports
- Clearly set out the minimal required content, including relevant facts and figures, to be included in the annual report



Continually review and update the governance framework

- Schedule regular reviews and updates of the BWC governance framework to ensure continued alignment with the guiding principles and purposes of the program
- Update policies and procedures in light of PIA results, audit findings and new academic research or expert findings
- Include ongoing opportunities to further consult with, and engage, relevant stakeholders and members of the public

Model Governance Framework for Police Body-worn Camera Programs in Ontario



Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

2 Bloor Street East,
Suite 1400
Toronto, Ontario
Canada M4W 1A8

www.ipc.on.ca
416-326-3333
info@ipc.on.ca

June 2021

GUIDANCE FOR THE USE OF BODY-WORN CAMERAS BY LAW ENFORCEMENT AUTHORITIES



This guidance document aims to identify some of the privacy considerations law enforcement authorities should take into account when deciding whether to outfit law enforcement officers with body-worn cameras. Also described is the privacy framework that should be part of any law enforcement body-worn camera program in order to ensure compliance with Canada's personal information protection statutes.

This document is endorsed by:

Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of Alberta

Office of the Information and Privacy Commissioner for British Columbia

Manitoba Ombudsman

Office of the Access to Information and Privacy Commissioner - New Brunswick

Office of the Information and Privacy - Newfoundland and Labrador

Office of the Information and Privacy Commissioner of the Northwest Territories

Nova Scotia Freedom of Information and Protection of Privacy Review Office

Office of the Information and Privacy Commissioner of Nunavut

Office of the Information and Privacy Commissioner of Ontario

Office of the Information and Privacy Commissioner of Prince Edward Island

Commission d'accès à l'information du Québec

Office of the Saskatchewan Information and Privacy Commissioner

Office of the Yukon Information and Privacy Commissioner



Guidance for the use of body-worn cameras by law enforcement authorities

Introduction

This guidance document aims to identify some of the privacy considerations law enforcement authorities¹ (LEAs) should take into account when deciding whether to outfit law enforcement officers with body-worn cameras (BWCs). Also described is the privacy framework that should be part of any law enforcement BWC program in order to ensure compliance with Canada's personal information protection statutes. This guidance is meant to support LEAs in developing policies and procedures governing the use of BWCs. It relates to the *overt* use of BWCs, that is, BWCs that are used in view of the public and with the understanding that the public has been informed of their deployment. The covert use of BWCs is not addressed through this guidance.

This document was developed by the Office of the Privacy Commissioner of Canada in collaboration with the privacy oversight offices in [Alberta](#), [New Brunswick](#), and [Quebec](#) and in consultation with the privacy oversight offices in [British Columbia](#), [Manitoba](#), [Newfoundland and Labrador](#), [Northwest Territories](#), [Nova Scotia](#), [Nunavut](#), [Ontario](#), [Prince Edward Island](#), [Saskatchewan](#) and [Yukon](#).


Apart from requirements under personal information protection statutes, the use of BWCs can implicate other obligations of which LEAs need to be aware. For example, BWCs can record video images, sound and conversations with a high degree of clarity. Thus, there may be additional concerns raised under the *Canadian Charter of Rights and Freedoms*, the *Criminal Code*, or provincial legislation², for example, whether the use of BWCs in any given context intrudes on the public's reasonable expectation of privacy or constitutes an interception of private communications, including in places accessible to members of the public. LEAs also need to be mindful of additional legal implications whenever images and sound are recorded in private spaces, such as inside people's homes or vehicles.

BWCs and privacy

BWCs are recording devices designed to be worn on a law enforcement officer's uniform, which can include glasses or helmets. They provide an audio-visual record of events from an officer's point of view as officers go about their daily duties. The high-resolution digital images allow for a clear view of individuals and are suited to running video analytics software, such as facial recognition. Microphones may be sensitive enough to capture not only the sounds associated with the situation being targeted but also ambient sound that could include the conversations of bystanders.

¹ This constitutes government agencies responsible for enforcing laws and includes, but is not limited to, police forces.

² For example, in Québec, the *Charter of Human Rights and Freedoms* or the *Civil Code of Québec*.



BWC technology represents a significant increase in sophistication from the early days of fixed cameras, when CCTV systems were being widely adopted and could only record images and not sound. At that time, a number of Canadian privacy oversight offices issued video surveillance guidelines for the public sector, which are set out at the end of this document. While the basic privacy principles around video surveillance remain the same, the environment is now much more complex. As surveillance technologies evolve, ever larger amounts of personal information (both video and audio) are being collected in increasingly diverse circumstances (both static and mobile) with the potential of being linked with yet other personal information (e.g. facial recognition, metadata). It is understandable that LEAs would want to consider using new technologies to aid them in performing their duties. At the same time, however, BWC technology poses serious implications for individuals' right to privacy. We believe that addressing privacy considerations from the outset can allow an appropriate balance to be achieved between the needs of law enforcement and the privacy rights of individuals.

Body-worn cameras capture personal information

Canadian personal information protection statutes generally define personal information as being “about an identifiable individual.”³ Under Québec’s *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information*, personal information is “any information which relates to a natural person and allows that person to be identified.”

Generally speaking, the aim of a BWC program is to record law enforcement officers’ interactions with the public in the course of their duties. BWCs are generally used for collecting evidence, and protecting officers against unfounded allegations of misconduct. Another significant argument for BWCs is enhancing officer accountability and professionalism. Given this context, and the increasing quality of recordings and sensitivity of microphones, the images and sound captured by BWCs for the most part will be about identifiable individuals. The recordings will thus be considered to contain personal information and will be subject to Canada’s personal information protection statutes.


In addition to images and sound, BWCs can also generate metadata, which can include transactional information about the user, the device and the activities taking place. Metadata can include date, time, location and duration of the recorded activities, which, when connected to an identifiable individual, can be personal information⁴.

What is the right balance between privacy and law enforcement needs?

There are various reasons why a LEA might contemplate adopting BWCs. LEAs could view the use of BWCs as bringing about certain benefits to policing or other enforcement activities. For

³ The case law at the federal level has generally held that information will be about an identifiable individual if it permits or leads to the possible identification of the individual, whether alone or in combination with other available information.

⁴ For further information on metadata, please see the Ontario OIPC’s [“A Primer on Metadata: Separating Fact from Fiction”](#) and/or the OPC’s [“The Risks of Metadata”](#)



example, in addition to being used to collect evidence, BWCs have been [associated with](#) a decrease in the number of public complaints against police officers as well as a decrease in the use of force by police officers. At the same time, BWCs have significant privacy implications that need to be weighed against the anticipated benefits. As the Supreme Court of Canada has noted⁵, an individual does not automatically forfeit his or her privacy interests when in public, especially given technological developments that make it possible for personal information “to be recorded with ease, distributed to an almost infinite audience, and stored indefinitely”. And as the Supreme Court added more recently, the right to informational privacy includes anonymity which “permits individuals to act in public places but to preserve freedom from identification and surveillance.”⁶

The use of BWCs inside private dwellings brings up special considerations, such as the higher likelihood that individuals will be recorded in highly personal situations. Before proceeding with a BWC program, LEAs should identify their lawful authority for collecting personal information using BWCs. Generally, under public sector personal information protection statutes, public bodies may only collect the information they need to meet the purposes of their mandated programs and activities. As a second step, LEAs should evaluate whether the anticipated benefits of adopting BWC technology outweigh the resulting privacy intrusions. In other words, is it appropriate to equip officers with cameras given the privacy implications they raise?

Privacy oversight offices have found it useful to use a four-part test to evaluate whether a proposed measure can be justified despite an intrusion on individual privacy. The test of “what a reasonable person would consider appropriate in the circumstances” provides a useful basis for LEAs in setting out the rationale for adopting BWCs. LEAs should be guided by this four-part test as set out below in determining whether to implement BWCs.

Necessity

There must be a demonstrable operational need that a BWC program is meant to address. What operational needs do LEAs have for which BWCs are a solution?

BWCs should not be adopted simply because they may be considered a popular enforcement tool. They must be judged necessary to address specific operational circumstances in the jurisdiction they are deployed in.

Effectiveness

Are BWCs likely to be an effective solution to the operational needs that have been identified? LEAs should be mindful of the limitations of technology. Aspects of incidents may happen out of camera range, sound recordings may be incomplete due to range or background noise, or human error may compromise the usefulness of recordings and diminish their effectiveness. If recordings are meant to be used as evidence in court proceedings, LEAs should consider the requirements identified by Courts for accepting recordings as evidence as well as the evidence collection and retention measures proposed to ensure those requirements are satisfied.

⁵ *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62 at para. 27.

⁶ *R. v. Spencer*, 2014 SCC 43



Proportionality

Without a doubt, the use of BWCs will result in a loss of privacy because recording individuals' actions and conversations is inherently privacy invasive. As such, any privacy intrusion must be minimized to the extent possible and offset by significant and articulable benefits. With new technology, it may be difficult to foresee the full spectrum of positive and negative effects on day-to-day enforcement and the community being served. Undertaking a pilot project is highly recommended as a practical way of evaluating the privacy impacts of BWCs in relation to their benefits, before deciding whether or not to deploy them, how broadly, and in what circumstances.

Alternatives

A final consideration is whether a less privacy-invasive measure would achieve the same objectives. While there may be a business case for a BWC program, alternative measures should be considered to see whether they can adequately address operational needs with less adverse impact on privacy. The least privacy invasive measure is the preferred choice.

Privacy Impact Assessments


As a highly recommended best practice, a Privacy Impact Assessment (PIA) should be completed prior to the use of BWCs to help identify the potential privacy risks of the BWC program. A PIA can be invaluable in helping LEAs eliminate those risks or reduce them to an acceptable level. For example, there may be additional considerations, such as context and cultural sensitivities, that should be considered in deciding whether to use BWCs in particular situations. A PIA should include a plan for consulting and engaging with the community where BWCs are to be deployed.

LEAs can also seek the aid of privacy experts before implementing a BWC program. Privacy experts can study the proposed use of BWCs in the community to ensure that any collection and use of personal information is done with a view to upholding obligations under privacy legislation.

Secondary uses

Employee privacy should also be taken into account. BWCs can capture law enforcement officers' personal information, which is protected under most public sector privacy laws. Potential areas of concern include using BWC recordings to support employee performance evaluations. Employees may also have privacy rights under other laws and collective agreements that may affect a BWC program.

If use of recordings is contemplated for any purposes that are supplementary to the main BWC program purposes, for example, officer training, research, or performance evaluation, these secondary purposes need to be reviewed to ensure compliance with applicable legislation, and employees need to be well informed of them. In addition, criteria should be established to limit



the privacy impact, such as blurring of faces and any identifying marks, and excluding recordings with sensitive⁷ content.

Pilot projects

The considerations in implementing a BWC program are complex, and pilot projects are recommended as an important precursor to widespread adoption. It is generally good practice, when deploying new technologies, to try them out in the field on a limited basis. If a LEA decides that adopting BWCs is appropriate, a pilot project would demonstrate how BWCs actually perform in their specific environment and whether this technology produces useful results that satisfy the intent of the program. The pilot project could also inform the crafting of a clear policy framework, applicable training requirements, and required supervision.

Evergreening PIAs

After a BWC program has been adopted, additional PIAs are recommended as a best practice any time significant modifications to the program are contemplated. Significant modification would include a new collection of personal information and the introduction of new technologies or analytical tools.

Notifying the public


LEAs should make a reasonable effort to inform the public that officers are equipped with BWCs and that people's actions and words may be recorded when they interact with, or are in the vicinity of, law enforcement officers. Transparency is integral to the public's ability to exercise their rights under privacy laws.

Public awareness of the use of BWCs can be raised through the local media, social media campaigns, and on LEA websites. Individuals should be advised if BWCs are used, for what purpose, in what circumstances, under what authority and who they can contact in case of questions. As part of their commitment to fostering public awareness, LEAs should consider reminding the public that individuals have a right to access their own personal information, as well as a right to request access to information generally under freedom of information laws that apply to BWC recordings.

Notification is also important in encounters between law enforcement officers and the public. Should non-uniformed officers use BWCs, there is an increased risk that the public will be unaware that recording may potentially take place.

While BWCs are visible on the officer's uniform or glasses, they may not be noticed by individuals, particularly in stressful situations. Individuals also may not be aware that sound is being recorded in addition to images.

⁷ LEAs should determine criteria for designating sensitive content, with input from the affected community, and ensure a higher level of protection for such recordings.



Law enforcement officers should be required to notify people of recording both images and sound whenever possible. Officers could make a short statement that meets notice requirements under applicable legislation in their jurisdiction. A prominent pin or sticker on the officer's uniform could also be an option depending on the circumstances.

Continuous versus intermittent recording

One of the most important operational decisions LEAs must make in implementing a BWC program is whether BWCs should record continuously or whether officers should have the discretion or duty to turn them on and off, and, in either scenario, under what circumstances. These choices have important implications for privacy.

From an accountability perspective, continuous recording may be preferable because it captures an unedited recording of an officer's actions and the officer cannot be accused of manipulating recordings for his or her own benefit. However, from a privacy perspective, collecting less or no personal information is always the preferred option. The less time BWCs are turned on, the less personal information they will collect. Minimizing the personal information collected decreases the risk that personal information will be used or disclosed for inappropriate or unintended purposes. This applies both to members of the public whose personal information is recorded by BWCs as well as law enforcement officers. There may be times during an officer's workday that having the camera turned on would not capture any information related to evidence collection or any other stated purpose of the BWC program, for example, when the officer is "standing by" or doing paperwork. LEAs also have a responsibility to respect officers' personal privacy when off-duty or on personal time. As for recording the public, LEA programs should take into account situations that merit heightened privacy protections, such as when officers enter private dwellings.


In general, it will be difficult for LEAs to justify the necessity of continuous recording. Recording may be more readily justified, however, in relation to carefully defined incidents or operational requirements.

If intermittent recording is implemented, there should be strict criteria for turning cameras on and off, including criteria for determining whether the officer should have control in turning the cameras on or off, or whether this should be done remotely.

The criteria developed should take into account fundamental freedoms, human rights, cultural sensitivities and any significant concerns expressed by the affected community.

Try to avoid recording bystanders

The criteria for activating cameras should address the need to minimize, to the extent possible, the recording of innocent bystanders or innocuous interactions with the public. Admittedly, it may not be possible to completely eliminate capturing images and audio of bystanders and other non-targeted individuals. With regard to recordings that are not implicated in an investigation (i.e. non-flagged recordings), setting and respecting limited and appropriate retention periods, and restricting access and viewing to a need-to-know basis will help mitigate the privacy implications.



With regard to recordings that have been flagged for use as evidence or for another previously specified purpose, technical means should be employed to mitigate the privacy risk. Within the rules of evidence, and in particular, the jurisprudence with respect to the reliability of evidence, images of bystanders and other non-targeted individuals should be anonymized, for example, through face blurring, and the distortion of sound wherever possible.

If images and/or audio are shared with the public for the purpose of identifying someone, other persons in the images should be obscured, with measures taken to safeguard the evidentiary integrity and reliability of the recording.

Proper safeguards, retention, destruction and storage of BWC recordings


Under privacy legislation, LEAs are responsible for protecting personal information from unauthorized access or use, disclosure, copying, modification and destruction, as well as loss and theft. Reasonable steps must be taken to safeguard recordings, such as:

- encrypt recordings and store them on a secure server;
- restrict access to recordings, on a need to know basis;
- edit-proof video and audio; and,
- implement an audit trail to provide assurance that recordings have not been modified or accessed inappropriately.

LEAs contemplating storing BWC recordings in the cloud should be mindful of potential security concerns as well as any legal constraints that may apply in their jurisdiction. For example, British Columbia's *Freedom of Information and Protection of Privacy Act* and Nova Scotia's *Personal Information International Disclosure Protection Act* may not allow public bodies to store personal information outside of Canada. Québec's *Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information* imposes certain conditions on the storage of personal information outside the province.

In light of the significant privacy implications of BWCs, strict retention periods should be imposed, taking into account the requirements of all applicable legislation. Setting and respecting retention periods will limit any opportunities for inappropriate disclosure or misuse of the information, including the potential for monitoring individuals without reasonable suspicion or probable cause.

Retention policies for flagged recordings, including recordings to be used as evidence, should be consistent with applicable laws, such as the *Canada Evidence Act* and the applicable *Police Services Act*. Under Canada's privacy laws, personal information that has been used in making a decision affecting an individual needs to be retained for a sufficient period so as to afford individuals a reasonable opportunity to access it and challenge its accuracy. Recordings that have not been flagged as relevant to an investigation or potential legal action should have the shortest possible retention period.



When the retention period is up, recordings should be disposed of in a secure manner in accordance with applicable policies⁸ and regulations.

There should be systems in place to ensure that safeguarding, retention and destruction policies are respected.

Use of video analytics

Any plans to use video analytics in conjunction with BWCs should be carefully considered with regards to the initial justification of the program. With advances in technology, we are gaining increasing ability to search and analyze digital footage in increasingly sophisticated ways. Databases of camera footage can be mined for information about specific individuals or specific activities. Previously anonymous individuals can be identified and tracked.

Technologies such as licence plate recognition, facial recognition and pattern recognition can be used in identifying, tracking and compiling dossiers on individuals. LEAs' use of video analytics technology raises additional privacy concerns that require further scrutiny and care beyond the scope of this guidance.

At this time, we simply observe that if the use of such analytics can be justified under privacy laws, the capability to analyze recordings must be carefully managed so as not to exceed the documented purposes of the BWC program. Integrating recordings with video or audio analytics should only be considered on a case-by-case basis, under very limited circumstances to be determined by the head of the LEA involved, and subject to a new PIA as necessary.

Individual access

Federal, provincial and territorial privacy laws grant individuals a right of access to their personal information, including that contained in audio and video recordings made using BWCs. This right is subject to specific exemptions such as law enforcement and investigation.⁹ Under freedom of information legislation, individuals have the right to request access to information held by public bodies. LEAs should establish a process for responding to requests for information contained in BWC recordings. When providing access, care should be taken to ensure that the personal information of individuals other than the requester, such as their image and/or voice, wherever possible, is protected.

⁸ At the federal level, please refer to Community Security Establishment's IT Security Guidance document "[Clearing and Declassifying Electronic Data Storage Devices](#)" and the OPC's "[Personal Information Retention and Disposal: Principles and Best Practices](#)." In Québec, please see the "[Guide to the destruction of documents that contain personal information](#)" published by the Commission d'accès à l'information du Québec.

⁹ Please address any questions about specific exemptions to the privacy oversight office in your jurisdiction.



Documenting policies and procedures


As part of any BWC program, LEAs should establish written policies and procedures that clearly identify the program objectives and set out the rules governing the program. These policies and procedures should include the elements listed below.

Governance and accountability

- The rationale for deploying BWCs, including the program purposes and operational needs.
- The legislative authorities for collecting personal information under the program.
- Roles and responsibilities of staff with regard to BWCs and their recordings.
- Criteria for context-specific continuous recording and/or turning BWCs on and off, as applicable.
- Provision for an operational guide and training for employees to ensure that officers understand the privacy implications of BWCs and are aware of their responsibilities under these policies and procedures.
- Privacy protections for employees whose personal information is captured by BWCs.
- The allocation of responsibility for ensuring that BWC policies and procedures are followed, with overall accountability resting with the head of the organization.
- The consequences of not respecting the policies and procedures.
- Individuals' right of recourse. Individuals should be informed that they have a right to make a complaint to the LEA's privacy oversight body regarding the management of a recording containing personal information to determine whether a breach of privacy law has occurred.
- The requirement that any contracts between LEAs and third-party service providers specify that recordings remain in the control of LEAs and are subject to applicable privacy laws.
- A provision for regular internal audits of the BWC program to address compliance with the policy, procedures and applicable privacy laws. The audit should include a review of whether BWC surveillance remains justified in light of the stated purposes of the program.
- In jurisdictions with a PIA policy, a provision for PIAs whenever there are significant modifications to the program.
- The name and contact information of an individual who can respond to questions from the public.

Use and disclosure of recordings

- The circumstances under which recordings can be viewed. Viewing should only occur on a need-to-know basis. If there is no suspicion of illegal activity having occurred and no allegations of misconduct, recordings should not be viewed.
- The purposes for which recordings can be used and any limiting circumstances or criteria, for example, excluding sensitive content from recordings being used for training purposes.
- Defined limits on the use of video and audio analytics.

- 
- The circumstances under which recordings can be disclosed to the public, if any, and parameters for any such disclosure. For example, faces and identifying marks of third parties should be blurred and voices distorted wherever possible.
 - The circumstances under which recordings can be disclosed outside the organization, for example, to other government agencies in an active investigation, or to legal representatives as part of the court discovery process.

Safeguards and response to breaches

- The security safeguards employed to ensure that recordings are not inappropriately accessed or altered.
- A mechanism for dealing with any breaches whereby personal information is accessed without authorization or disclosed contrary to the provisions of applicable privacy laws.

Access to recordings by individuals

- A process for responding to requests for access¹⁰ to recordings, including access to personal information and access to information requests under freedom of information laws, as well as individuals' requests for correction of their personal information. This includes the name and contact information of the individual to whom such requests for access to should be directed.

Retention and destruction of recordings

- Retention periods and disposal provisions.

These policies and procedures should be made available to the public to promote transparency and accountability. Demonstrating to the public that policies and procedures exist and officers are accountable for following them is essential to ensuring that individuals' privacy rights are adequately protected. The documentation should also reflect evidence of community consultation and engagement as well as an understanding of cultural sensitivities.

Conclusion

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

¹⁰ LEAs should have the capability to redact third party personal information to facilitate access, for example, blurring of faces.



References

Tony Farrar and Dr. Barrar Ariel. [“Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force,”](#) Police Foundation, March 2013.

David A. Harris. [“Picture this: body worn video devices \(“Head cams”\) as tools for ensuring fourth amendment compliance by police,”](#) University of Pittsburgh School of Law, April 2010.

The Honourable Frank Iacobucci. [“Police Encounters with People in Crisis,”](#) An independent review conducted for Chief of Police William Blair, Toronto Police Service. July 2014.

Police Executive Research Forum. [“Implementing a Body-Worn Camera Program.”](#) U.S. Department of Justice, Community Oriented Policing Services, 2014.

Jay Stanley. [“Police Body-Mounted Cameras: With Right Policies in Place, a Win For All,”](#) ACLU, October 2013.

The Urban Institute Justice Policy Center. [“Using Public Surveillance Systems for Crime Control and Prevention: A Practical Guide for Law Enforcement and Their Municipal Partners,”](#) September 2011.

U.K. Home Office. [“Surveillance Camera Code of Practice,”](#) June 2013.

U.S. Department of Justice. [“A Primer on Body-Worn Cameras for Law Enforcement,”](#) Office of Justice Programs, National Institute of Justice, September 2012.

Public sector video surveillance guidance from Canadian privacy oversight bodies

Office of the Information and Privacy Commissioner for British Columbia. “[Public Sector Surveillance Guidelines](#),” 2014.

Office of the Information and Privacy Commissioner of Saskatchewan. “[Guidelines for Video Surveillance by Saskatchewan Public Bodies](#).”

Office of the Information and Privacy Commissioner of Ontario. “[Guidelines for the Use of Video Surveillance Cameras in Public Places](#),” 2007.

Commission d'accès à l'information du Québec. “[Rules for use of surveillance cameras with recording in public places by public bodies](#),” June 2004.

Office of the Access to Information and Privacy Commissioner of New Brunswick. “[Best Practice – Video Surveillance](#),” April 2014.

Office of the Information and Privacy Commissioner for Newfoundland and Labrador. “[Guidance for the Use of Video Surveillance Systems in Schools](#),” February 2013.

Office of the Information and Privacy Commissioner for Newfoundland and Labrador. “[Guidelines for Video Surveillance by Public Bodies in Newfoundland and Labrador](#),” May 2005.

Nova Scotia Freedom of Information and Protection of Privacy Review Office. “[Freedom of Information and Protection of Privacy Review Office Video Surveillance Guidelines](#).”

Office of the Yukon Information and Privacy Commissioner. “[Guidance for Public Bodies on the Use of Video Surveillance](#),” 2014

Office of the Privacy Commissioner of Canada. “[OPC Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities](#),” March 2006.