JUNE 2021

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

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 systems[4] 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 so[9]

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 **Know0our 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 investigation[12]
- 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 blurring[13] 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 accidently 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

- ☐ 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