Portland Police Bureau
Body worn cameras.
Privacy Impact and Risk Analysis
FINAL VERSION

Smart City PDX
December 14, 2023

PRIVACY ANALYSIS REPORT

City of Portland Privacy Toolkit

WHAT IS THE PRIVACY ANALYSIS?

The Privacy Impact Analysis ("PIA") is a method to quickly evaluate what are the general privacy risks of a technological solution or a specific use, transfer, or collection of data to City bureaus or offices. The PIA is a way to identify factors that contribute to privacy risks and lead to proper strategies for risk mitigation or alternatives that may even remove those identified risks.

The Privacy Impact Analysis may lead to a more comprehensive Impact Assessment and a Surveillance Assessment depending on the level or risks identified and the impacts on civil liberties or potential harm in communities.

In the interests of transparency about data collection and management, the City of Portland has committed to publishing all Privacy Assessments on an outward facing website for public access. PIAs do not include specific uses of technology or data other than those initially evaluated.

WHEN IS AN PRIVACY IMPACT ANALYSIS RECOMMENDED?

A PIA is recommended when:

- A project, technology, data sharing agreement, or other review has been flagged as having some privacy risk due to the collection of private or sensitive data.
- A technology has high financial impact and includes the collection, use or transfer of data by city bureaus or third parties working for or on behalf of the city.

HOW TO COMPLETE THIS DOCUMENT?

City staff complete two documents:

- *The Privacy Analysis form.* This document identifies all important information related to the project description, data collection, use, safekeeping, and management; as well as a verification of existing privacy policies and measures to protect private information.
- *The Privacy Risk Assessment.* This document breaks the privacy risk into six different areas of evaluation: (1) Individual Privacy Harms; (2) Equity, Disparate Community Impact; (3) Political, Reputation & Image; (4) City Business, Quality & Infrastructure; (5) Legal & Regulatory; and, (6) Financial Impact. Then compares risks to the likelihood of happening to create a single risk measure based on the worst-case scenario.

Executive summary

This privacy impact assessment looks at the use of body worn cameras by Portland Police Bureau. The first section of this report includes general information about how these devices are going to be used by officers and describes how collected information or footage will be managed, including a description of the privacy and information protection safeguards in these systems.

This analysis is not necessarily linked to any specific vendor but focuses more on existing policies that the Portland Police Bureau has developed and implemented to manage and use body worn cameras and their information management systems.

The worst-case scenario identifies a **MEDIUM level risk**. We have identified most of the risks as individual privacy harms and political reputation and image. Several High-risk issues are connected to either unauthorized disclosure of information, misuse, or abuse of devices, and tampering with records or logs from high public interest events or situations.

Impacts from these risks would mostly be felt by individuals and their relatives whose information has been disclosed or modified without proper authorization. As a result, the political reputation and public trust of the City and Portland Police Bureau can be negatively impacted in those cases.

This analysis reinforces currents practices like proper training of everyone involved in using and managing these devices or their management systems (*Risk 1.2*). Portland Police Bureau is already doing these trainings and facilitating the proper use of body worn cameras and upload of footage.

To ensure fairness and proper due diligence of evidence and officer behavior, footage and records need to be preserved, and the integrity of those records maintained. This report recommends restricting officers' and supervisors' access to editing entries of footage (*Risk 2.2*). Supervisors do not lose access to entries; however, every edit gets logged in the system and available for audits. This strategy may reduce the risk of changing evidentiary value of footage and even unauthorized releases (*Risk 3.1*).

Finally, this report also recommends publicly accessible, well-documented and regularly scheduled audits, particularly those provided by neutral third parties (*Risk 5.1*). The public release of reports of usage, performance measures, and audits can improve performance and public trust through transparency and accountability (*Risk 5.3*).

This assessment was completed on November 20, 2023.

Privacy Impact Analysis

Purpose of the technology, project, data sharing or application

The Portland Police Bureau has adopted Body-Worn Cameras to accomplish several objectives, including: allowing for additional documentation of police-public contacts, encounters, arrests, and critical incidents; serving as a supplement to and/or enhancing the accuracy of officer reports and testimony; gathering evidence for investigative and prosecutorial purposes; providing additional information for officer evaluation, feedback, and training; and conducting fair and thorough professional standards reviews and investigations in resolving community/public and Bureau complaints. The use of BWC in this pilot program was approved by Portland City Council in the emergency ordinance 191257.

Name of the entity owner of the application and website

Portland Police Bureau
https://www.portland.gov/police/community/body-worn-camera-project

Type of Organization

Government

Scope of personal data collected. List all sources of data and information.

A law enforcement officer who is in uniform and displaying a badge and who is operating a video camera worn upon the officer's person that records the officer's interactions with members of the public while the officer is on duty.

The uniquely intrusive nature of police recordings made inside private homes, officers should be required to be especially sure to provide clear notice of a camera when entering a home, except in circumstances such as an emergency or a raid. Departments might also consider a policy under which officers ask residents whether they wish for a camera to be turned off before they enter a home in non-exigent circumstances.

Officers need to upload recordings manually. When uploading footage, members tag each recording in accordance with training (e.g., call type, citation or warrant number and, when applicable, the associated report number). There is also an auto-tag option available. it updates every 6 hours and will enter the Report number and a basic category (for retention). The officers are required to validate that information is correct during their next shift.

Bureau-purchased body-worn cameras do not allow for tampering with, manipulating, or altering content, or deleting recordings. Members are forbidden to tamper with, manipulate, or alter content or delete recordings.

Automated decision systems (ADS) are limited to certain areas like enhanced information from live or recorded footage or blurring faces or images that impact an individual's privacy. However, ADS available for body worn cameras footage processing can include automatic speech recognition, context and scenery recognition, face, or emotional state recognition, assessing or detecting objects, behaviors, people, and vehicles of concern.

Body-worn cameras need to be deactivated on specific circumstances:

- When there are victims of sexual assault, trafficking, or child abuse.
- When inside a courthouse, with exceptions.
- During communications between a suspect and their legal representation that would have a reasonable expectation of privacy unless activation is required under City Policy or required by law.
- During encounters with undercover members or confidential informants when discussing confidential information.
- When present in restricted areas of law enforcement facilities that are not routinely accessible to the public, not including intoxilyzer rooms, holding cells or interview rooms.
- In death notifications.

Body worn cameras may also collect geolocation information in addition to the timestamp.

How personal data is collected.

Footage capture by the cameras and their case reports drafted by members or wearing those devices. These reports may include case numbers, personal names, personal addresses, situational context, and narrative of events involving individuals.

Personal information may be collected by automatic decision systems postprocessing footage. These ADS can include automatic license plate readers, speech, or mental state recognition systems. Face recognition for identification purposes is forbidden in Portland.

Who can access the data?

In addition to the officer wearing the body-worn camera, the recording will have a list of reviewers:

- Supervisor and After-Action Review
- Performance Review
- Training Division Review
- Administrative Investigator Review
- Criminal Investigator Review
- Discovery of Misconduct During a Review

The Records Division is authorized to copy, share, or publicly release BWC recordings. Supervisors can share recordings. This is usually done with Detectives for follow-up, other agencies if PPB assisted on their call.

The Records Division shall receive and manage all public records requests for body-worn cameras recordings and act in accordance with state law regarding disclosure requirements. The Records Division will share information to the District Attorney

Prior to disclosure, Portland Police Bureau shall edit the video in a manner as to render the faces of all persons within the recording unidentifiable. The Bureau may make additional redactions in accordance with other exemptions permitted by law.

Bureau Body-Worn Camera Program Manager can perform periodic audits of BWC recording.

Purposes the data is used for.

Footage recorded by the body worn cameras can be used:

- As evidence in an ongoing investigation by administration or in criminal cases.
- To supervise activities in after-action reviews.
- To review performance of officers and actions.
- To train officers.
- To discover or review any misconduct.

Where the data is stored

The video and the metadata are uploaded to the PPB cloud site provided by the vendor. The vendor does not have access to PPB's evidence data without explicit authorization.

How data is shared

Video and metadata are shared through authorized members using the vendor's cloud services. Oversight and audits will be performed by the body-worn camera project manager.

The Records Division responds to requests of information from the public, agencies, and the District attorney, in accordance with state law regarding disclosure requirements. Supervisors can directly share information to detectives and other agencies in a specific case.

Prior to disclosure, the Bureau shall edit the video in a manner as to render the faces of all persons within the recording unidentifiable.

The Bureau may make additional redactions in accordance with other exemptions permitted by law. Including nudity, children, or images of dead bodies.

Images of a dead body, or parts of a dead body, that are part of a law enforcement agency investigation, if public disclosure would create an unreasonable invasion of privacy of the family of the deceased person, unless the public interest by clear and convincing evidence requires disclosure in the particular instance.

How long is the data stored?

ORS 133.741 § (1)(b)(A) requires that '… a recording be retained for at least 180 days but no more than 30 months for a recording not related to a court proceeding or ongoing criminal investigation, or for the same period of time that evidence is retained in the normal course of the court's business for a recording related to a court proceeding.'

Recordings are stored in the vendors cloud services site.

Effectiveness

Under the PPB BWC Policy, "Although BWC recordings have evidentiary value, they may not capture the entirety of an incident or the actual vantage point of the Bureau member, and footage may not necessarily depict the entire scene, circumstances, or incident in the way that it may have been perceived or experienced by any person present. BWC recordings serve as additional evidence related to an incident, but the footage is only an individual piece of evidence and should not be used in lieu of a complete and thorough police report or a complete and thorough investigation of any incident. Persons reviewing BWC recordings must be cautious before reaching conclusions about what the recordings show."

The video collected by the body worn cameras has limitations due constraints of the field of view of the device and does not represent the perception that the officer has of the events.

Human reaction to situations that officers experience in the field will influence the speed and ability to operate the device manually. Certain cases of automation are enabled, including activating emergency vehicle lights, and drawing their firearm or Conducted Electrical Weapon (CEW or teaser).

The City of Portland and the Portland Police Union recognize that the inability to review video can impact reporting accuracy. Both parties recognize that officers may not be able to recall at the time they are writing the report all information they in fact perceived that may be salient to the incident. Footage may not completely coincide with the officers' report.

The value of a body worn camera recording footage as evidence will be assessed by reviewers in a criminal investigation or by the administration.

Proportionality, fundamental rights, frequency of the collection, and data protection and privacy issues line unintended data collection or processing.

The use of body worn cameras responds to a US Department of Justice requirement by Portland Police Bureau to use body worn cameras. ECF No. 286-4, DOJ Letter to City and PPB (Nov. 15, 2021).

The use of body worn cameras by Portland Police Bureau will follow Oregon's and other applicable Laws.

Civil liberties advocates have highlighted concerns about the use of body worn cameras. Body worn cameras capture large amounts of data about people beyond those interacting with the

police officer wearing a camera; these cameras are focused on areas in front of an officer, not on the officer him/herself.

Some issues identified with body worn cameras effectiveness are:

- Who and what should be recorded?
- When do officers hit “record”?
- When do officers hit “stop”?
- Are there any exemptions to recording?

Camera activation.

Officers wearing a body worn cameras need to be activated either automatically or manually. Cameras should be automatically activated when activate emergency vehicle lights on specific cases. Camera does not activate when their CEW is drawn. It does activate only on arcing or firing.

Cameras should be manually activated when:

- Dispatched or otherwise responding or “self-dispatching” to a call for service.
- Engaging with the public during a public order event, when consistent with the law.
- Attempting to conduct a traffic or pedestrian stop.
- Attempting to obtain consent for a search or conduct a search.
- Conducting a custodial interview of a juvenile outside of a law enforcement facility, when the person is under 18 years old and being interviewed in connection with an investigation into a misdemeanor or a felony, or an allegation that the person being interviewed committed an act that, if committed by an adult, would constitute a misdemeanor or felony.
- The member develops reasonable suspicion or probable cause to believe that a crime or violation has occurred, is occurring, or will occur and the member begins to contact the person suspected of committing the offense.
- When the Special Emergency Response Team (SERT) members arrive at a scene.

Officers may forget or not been able to activate the body worn camera and lose important footage of the specific action.

Important contextual evidence might not be recorded by body worn camera.

Under the current 2023 pilot policy for using the PPB Body Worn Cameras , "Although BWC recordings have evidentiary value, they may not capture the entirety of an incident or the actual vantage point of the Bureau member, and footage may not necessarily depict the entire scene, circumstances, or incident in the way that it may have been perceived or experienced by any person present. BWC recordings serve as additional evidence related to an incident, but the footage is only an individual piece of evidence and should not be used in lieu of a complete and thorough police report or a complete and thorough investigation of any incident. Persons reviewing BWC recordings must be cautious before reaching conclusions about what the recordings show."

Technological limitation of video collection limits what gets in the footage.

Video evidence has limitations and may depict the events differently than you recall and may not depict all the events as seen or heard by you. Video has a limited field of view and may not Video evidence be intended to assist your memory and ensure that your statements explain

your state of mind at the time of the incident. Capture events normally seen by the human eye may not be recorded by cameras. The frame rate of video may limit the camera's ability to capture movements normally seen by the human eye.

Advantages of using body worn cameras.
A camera may see better than people do in low light. Cameras can also register exact time of event; these timestamps may prove critical as evidence.

Privacy safeguards

In an interaction with an officer.
Oregon law describes how law enforcement agencies limits what can be recorded in video and audio and how vendors can access these information. Oregon Law also prohibits the use of facial recognition and other biometric matching technology using the camera.

An officer in someone's home.
In locations where individuals have a reasonable expectation of privacy, such as a residence, individuals may decline to be recorded or request that an officer not record them. Officers will evaluate each situation and when appropriate, may honor the individual's request. However, officers have no obligation to stop recording in response to the request if the recording involves an investigation, arrest, lawful search, or the circumstances clearly dictate that continued recording is necessary.

Residents' expectations of privacy.
Prior to disclosure, the Bureau's Records group will edit the video in a manner to render the faces of all persons within the recording unidentifiable.

The Bureau may make additional redactions in accordance with other exemptions permitted by law.

Officers' expectation of privacy.
Police officers themselves also have a right to privacy, and bodycams could make some important parts of their jobs more difficult. Use, operation, and reviews of individual body worn cameras may generate data used to evaluate performance of individual officers.

Open source

Not applicable

AI/ML claims

No.

Privacy Policy (link)

Not applicable. Oregon Law references:

• ORS 133.402 Recording of Custodial Interviews of Juveniles (https://oregon.public.law/statutes/ors_133.402)
• ORS 133.741 Law Enforcement Agency Policies and Procedures Regarding Video and Audio Recordings (https://oregon.public.law/statutes/ors_133.741)
• ORS 165.540 Obtaining Contents of Communications (https://oregon.public.law/statutes/ors_165.540)
• ORS 181A.250 Specific Information Not To Be Collected or Maintained (https://oregon.public.law/statutes/ors_181a.250) – This law does not exempt gender identity, race, ethnicity, disability, or medical status.
• ORS 192.345 Public Records Conditionally Exempt from Disclosure (https://oregon.public.law/statutes/ors_192.345)
• ORS 192.355 Public Records Exempt from Disclosure (https://oregon.public.law/statutes/ors_192.355)
• ADM 8.03 Public Records Requests (https://www.portland.gov/sites/default/files/policies/adm-8.03-public-records-request-new-contact-list-added.pdf)
• DIR 0310.70, Dissemination of Information (https://www.portlandoregon.gov/police/article/525547)
• DIR 0317.40 Authorized Use of Bureau Resources (https://www.portlandoregon.gov/police/article/546637)
• DIR 0330.00, Internal Affairs, Complaint Intake and Processing (https://www.portlandoregon.gov/police/article/759428)
• DIR 0635.10, Crowd Management/Crowd Control (https://www.portland.gov/policies/police-directives/field-operations-0600/063510-portland-police-bureau-response-public)
• DIR 0640.36, Communicating with Hearing Impaired and Limited English Proficient Persons (https://www.portland.gov/policies/police-directives/field-operations-0600/064036-communication-hearing-impaired-and-limited)
• DIR 0900.00, General Reporting Guidelines (https://www.portland.gov/policies/police-directives/report-writing-0900/090000-general-reporting-guidelines)
• DIR 0910.00, Use of Force Reporting, Review, and Investigation (https://www.portland.gov/policies/police-directives/report-writing-0900/091000-use-force-reporting-review-and-investigation)
• DIR 0905.00, Non-Force After Action Reporting (https://www.portland.gov/policies/police-directives/report-writing-0900/090500-non-force-after-action-reporting)
• DIR 1010.00, Use of Force (https://www.portland.gov/policies/police-directives/weapons-ammunition-equipment-1000/101000-use-force)
• DIR 1010.10, Deadly Force and In-Custody Death Reporting and Investigation Procedures (https://www.portland.gov/policies/police-directives/weapons-ammunition-equipment-1000/101010-deadly-force-and-custody-death) - supervisory line and chain in command descriptions.

• DIR 1200.00 Inspections, Maintenance, Responsibility, and Authority (https://www.portland.gov/policies/police-directives/maintenance-vehicles-property-1200/120000-inspections-maintenance) – supervision and inspections description.

Privacy risk

Medium. Some risks need to be mitigated.

Surveillance Tech?

Yes

Portland Privacy Principles (P3)

Data Utility

Body worn cameras capture footage in their field of view and officers need to comply with rules on where to locate their cameras. There are some effectiveness issues, but approved policies are design to guide their use, operation, and maintenance.

Full lifecycle stewardship

Full vendor and bureau operation of body worn cameras and recorded footage has been considered. The legal framework mandates specific procedures and documentation of access and revisions of footage. Destruction of footage is also according to the law.

Transparency and accountability

Footage from recordings collected from body worn cameras will follow Oregon's Public Record Laws, including exemptions. Public Records Requests is the legal instrument to access recorded footage from body worn cameras.

Civil complaints trigger review of footage by a supervisor.

Ethical and non-discriminatory use of data

Body worn cameras will be used under Oregon Law. Police Bureau policy number PPB-0620.00 governs the use, procedures, and management of body worn cameras.

Data openness

Some performance measures have been discussed. These measures include how cameras affect the civility of officers and community members; reduction in the number of citizen complaints or expedite resolution of those complaints; reduction of overtime costs for court appearances based on guilty or no contest pleas; effects of cameras reducing use of force incidents.

Automated Decision Systems

Automatic processing of images is only used for enhancing the quality for investigative purposes. Automatic blurring of faces or sections in the footage that required obscuration will be done by the records division.

Applying Face recognition in live or recorded footage is not allowed [ORS 133.741 § (1)(b)(D)].

Consent.

Consent is a requirement in cases where the officer is interviewing victims of sexual assault, trafficking, or child abuse.

Privacy Impact Risk Severity Assessment

WORST CASE SCENARIO	MEDIUM RISK

1. Individual Privacy Harms

1.1 Recordings in private locations.

Risk of invasion of individual privacy by recordings in places or areas where cameras generally are not allowed or permissible (e.g., locker rooms, dressing rooms, medical facilities, restrooms, in facilities where recording is prohibited).

Likelihood: **Likely**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

- The use of body worn cameras is under legal exceptions based on reasonable privacy concerns, exigent circumstances or the safety of law enforcement officers or other persons [ORS 133.741 § (1)(c)].
- The PPB policy also allows certain exemptions to pause the recording: 'Members are authorized to enable sleep mode when engaging in personal private activities, such as using a bathroom or other similar conduct'. PPB-0620.00, Section 6.1.1.1.
- Officers need to be trained about these alternatives and when to identify a situation where privacy allows an exemption to the recording. Officers could keep recording if the conditions require it or pausing the video is not feasible.

1.2 People unaware of recordings.

There is a risk to individuals when they are near a law enforcement encounter, regardless of whether they are directly or indirectly involved.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

- According to the PPB policy, officers are required to notify about the recording: 'When contacting a person, members shall announce to the person at the beginning of the interaction that the member is recording the interaction, unless not feasible'. PPB-0620.00, Section 3.1.
- Certain situations may put officers under stress, leading to errors in camera operation. Officers should prepare and rehearse in training scenarios that emphasize procedures and informing people of the recording.

1.3 Records not accessible to people.

There is a risk that members of the public may not be able to access their records given the law enforcement nature of the activities captured in the audio and visual recordings.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

Timely public records request responses should be prioritized.

The records group is already trained in using video editing software for blurring faces and identifying private components in footage. However, proper staffing is also required.

Members of the public or media may feel entitled to have access to specific records; however, the bureau needs to communicate about existing protocols.

Publicly accessible information about procedures to protect privacy and inform records release procedures should be make available by the bureau.

1.4 Risk of over-exposing individuals or locations.

The risk is that Body Worn Cameras could capture images of individuals recorded in the proximity of an incident that are irrelevant to the interaction or encounter. These individuals may include witnesses, passers-by, covered officers, children, or schools, hospitals, or locations of cultural, religious, or historical meaning to specific communities.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

Records management team are tasked to blur faces.

Proper supervising procedures need to be in place to assure footage is properly processed before public release.

Automatic detection and redaction tools may help records management to protect sensitive information. These tools can include detection of faces.

Assisted indexing of certain types of events like fires, crowds, or explosions could also be done automatically. Automatic acoustic privacy filters may mask various environmental sounds.

On the use of automatic tools, it is important to highlight that the use of face recognition technology is forbidden in Portland, and other biometric visual identification tool may be subject to error and bias.

1.5 Risk of failing to deactivate a camera in required scenarios.

Even if a community member requests that an officer deactivate their BWC, the officer may not do so unless permitted by Bureau policy.

Situations in which camera deactivation is required include:

When interviewing victims of sexual assault, trafficking, or child abuse.

Unless doing law enforcement actions:

- When inside a medial or mental facility,
- When inside a courthouse.
- During communications between a suspect and their legal representation.

During encounters with undercover members or confidential informants.

When present in restricted areas of law enforcement facilities.

During death notifications.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

Officers should be familiar with the procedure for automatic and manual start/stop of recording and receive either a visual or audio clue that the camera is activated.

Proper documentation of how cameras are used should be reviewed by officers.

If officers unintentionally record footage in a context not allowed by the current policy, records management can still anonymize and constrain access following the law and regulations.

1.6 Unprovoked targeting of officers.

The risk is that members of the public could target officers unprovoked by using the officer's personal information. Officers may be exposed to targeting due to the nature of their work or public attention due to a specific case.

Likelihood: **Unlikely**
Impact: **Moderate**
Risk level: **Low**
Mitigation/Recommendations:

The public interest may require names of officers be released publicly. Transparency and accountability procedures are an essential part of public trust.

The bureau may be able to protect officers' names and other personally identifiable information according to the law and City procedures.

Release of properly managed body worn footage can clarify officers' behavior in a specific context or case. Officers need to wear and use their cameras as instructed to ensure the footage records their interactions with others.

2. Equity, Disparate Community Impact

2.1 The use of BWC biased against specific groups.

There is a risk of disproportional negative impacts of recording incidents involving officers and specific groups. The assumption is that the use of BWCs will reduce the number of complaints due to incidents with individuals who are part of a specific group or demographic.

Likelihood: **Possible**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Public trust is an important factor in the use of technology. Surveillance technologies have often been described as specifically targeting communities of color.

Rely on public education to inform about strategies to ensure anti-discrimination and responsible use of body worn cameras and footage.

The collection of demographic information from recordings is very difficult due to the limitations and nature of the footage, including issues around video quality. Also, extracting demographic information and its validations is impractical due to the amount of video recorded.

The bureau can explore using alternatives to assess impacts on specific groups. These strategies can include geographic metadata, police logs, and information from criminal cases describing race, ethnicity, and other demographics connected to those cases.

Performing deeper analysis on the level of interactions can also provide insightful information to the bureau about better ways to use technology and interact with people.

Natural language processing or other demographic data analysis tools that could show biases or discrimination against specific demographics, people with visible or invisible disabilities, people in mental distress or situations of vulnerability can help improve procedures on the use of body worn cameras and officers' protocols in interacting with the public.

The bureau could consider opening access to footage to researchers under confidentiality agreements, strict control, and specific goals to determine levels of social, psychological, or individual contexts that can help improve officers' interactions with the public and better use of technology in the context of law enforcement.

2.2 Biased revisions or editing of footage involving people of color.

The risk is that, due to the history of systemic racism, revisions and editing could harm and impact some groups more than others.

Officers or supervisors may be tempted to change original descriptions or narratives, particularly involving people of color or people in disadvantage situations. These revisions may impact the evidentiary value of the footage of an incident.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

The logs and registers of activities in the vendors system capture every single modification made by users (officers and supervisors). That history is available to the project manager and every modification generates a record.
officers' and supervisors' already have restricted access to footage. Supervisors once their original input is complete can provide better control to management authorities.
To assure better control on entries, officers and supervisors edits and modifications are logged and available in the audit trail. Any request for modifying entries should go up the authority chain. This strategy may reduce the risk of changing evidentiary value of footage and even unauthorized releases.
Further reviews of original inputs may affect the neutrality of the inputs; misrepresent evidence; and introduce practical, ideological, or social standpoints, biases, and constraints. Further analysis may help to understand limitations of the use of this technology.

3. Political, Reputation & Image

3.1 Abuse of "non-evidentiary" footage.

The risk is that recordings of "non-evidentiary" value could be shared with third parties that may misuse its content.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Intentional sharing of footage with third parties that may not be part of a specific case without the proper records management could result in privacy breaches or revealing officers' actions without proper supervision.
The risk of releasing footage collected in locations relevant to specific communities should be taken into consideration. They might include places of worship, schools, hospitals, and community centers and markets.

3.2 Misidentification of an individual solely from body worn camera footage.

The risk is that PPB could identify and take enforcement action against an individual based solely on a Body Worn Camera recording. Solely using BWC footage for enforcement could risk misidentification of an individual.

Likelihood: **Possible**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Identification of specific individuals solely from body worn camera footage can lead to errors.
With a default resolution of 720 high dpi, footage is clear for assessing general interactions; however, factors like lighting, shades, or footage stability may make difficult identification of individuals. Additional footage or information may be.
Identification of individuals should rely on law enforcement best practices assisted by intelligence information from witnesses.
Use of facial recognition is not allowed in Portland.

3.3 Misuse of BWC in fishing expeditions or for dragnet surveillance.

If police officers and prosecutors can analyze all this data without restrictions, the risk is that it could be used for fishing expeditions or for dragnet surveillance using facial recognition software. “Fishing expedition” refers to someone excessively investigating or demanding information from an individual or organization.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Officers and supervisors should have restricted access to footage just for their specific reporting or reviews. Supervisors should keep attention on proportionality of surveillance according to the investigation case..
Use of information sources for investigative purposes including face templates, biometric databases, and automatic analysis tools needs to be documented and reported.

3.4 Intelligence gathering or spying.

The risk is that officers might be tempted to use body worn cameras to gather information about how people exercise their First Amendment rights to speak, associate, or practice their religion.

Likelihood: **Unlikely**
Impact: **High**

Risk level: **Medium**
Mitigation/Recommendations:

Use of body worn cameras should be restricted to the scope of the PPB policy established for this technology.

Officers should make the best efforts to confirm that their body worn camera is recording and deactivate it in locations and situations described in the PPB policy.

4. City Business, Quality & Infrastructure

4.1 Camera may not start with auto-triggering.

The risk is that issues with auto-triggering a BWC could prevent the camera from starting recording.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

Equipment should be properly maintained, and officers should perform periodic checks of its functionality, including Bluetooth connectivity among equipment and onboard computers.
Officers need to feel confident that equipment won't fail in the field and that they understand situations where auto-triggering needs to happen.

4.2 Procedures not followed properly by officers.

The risk is that officers may not properly use procedures to assure good quality footage or uploading files timely.

Likelihood: **Unlikely**
Impact: **Moderate**
Risk level: **Low**
Mitigation/Recommendations:

Before using body worn cameras, officers need to feel confident in the proper use of the cameras.
Enforcement of training and rehearsing of complex situations will help to obtain faster and more effective responses by officers wearing these devices.
Officers need to make sure cameras are placed on proper locations on the officer's body and be functional.
Early feedback and supervising operations for constant improvement can increase effectiveness and individual confidence in the use of these devices.
Strategies for corrective actions need to be clear to officers and supervisors.
Constant internal communications will improve better operation of devices.

4.3 Purposely misuse body worn cameras.

The risk is that officers purposely sabotage body worn camera recording.

Likelihood: **Unlikely**

Impact: **High**

Risk level: **Medium**

Mitigation/Recommendations:

The risk of having an officer purposely misusing a device should be detected by any step in the supervising chain of authority.

As these devices are perceived as tools for public accountability of officers, public oversight and interest are expected.

The bureau should be prepared to allow access to footage involving police misconduct using proper institutional channels. Effective and timely response to public interest will increase trust and institutional credibility.

4.4 BWC information is not used for continuous improvement.

The risk is that body worn cameras do not provide the information to correct systemic problems or individual officer issues.

Likelihood: **Possible**

Impact: **Moderate**

Risk level: **Medium**

Mitigation/Recommendations:

One of the main purposes of this technology is to improve institutional and individual accountability.

The bureau needs to prepare metrics that represent how body worn cameras are contributing to the improvement of policing services, reductions of individual officers' misbehavior (in anonymized form), and effective use of police resources.

4.5 Inaccessible civil complaint.

The risk is that people who have potentially been mistreated by an officer cannot access footage to help with a civil complaint.

Likelihood: **Possible**

Impact: **High**

Risk level: **Medium**

Mitigation/Recommendations:

The effective and timely response to public complaints will improve public trust.

The bureau needs to facilitate public records services staff to respond to these requests.

At the same time, the bureau needs to inform people about these procedures, expected time of response, the limitations that the law prescribes for released footage, and where people can find additional information.

On the other hand, civil complaints may create stressful situations for officers, particularly when they have not done anything wrong. The bureau needs to develop ways to support training and assistance to officers in these situations.

4.6 Missing privacy protection of sections of publicly released footage.

The risk is that certain information released to the public is not properly blurred or protected, including situations that expose people's vulnerabilities or personal situations.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

The administrative use of this technology describes what elements need to be blurred or protected.
In responding to a public request for information, the records management team needs to make sure to follow the privacy protection process.
In some cases, some information may be hard to identify in live footage.
The use of auto-tagging software may need to be supervised to reduce the risk of implicit biases or mislabeling.

4.7 Video footage is low quality and images are not clear.

The risk is due to technical limitations or specific lighting conditions, officer movements, or camera lens conditions may create images that are not clear enough to use as evidence in a case.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

The default footage resolution is 720 high dpi, and the selection of this resolution was due to balancing the camera's battery charge and expenses in video storage.
The use of higher resolution would allow clearer and sharper images; however, the bureau should evaluate alternatives that allow higher resolution and rates of collection that still work with the existing battery charge.
Regular use of cameras may reduce battery life. Make sure regular maintenance includes battery checks, lenses clean up, and integrity of the device security features.
Specific training and procedures may need to be implemented to reduce this risk with officers.

5. Legal & Regulatory

5.1 Recording outside the scope of the law.

The risk is that PPB personnel could record video outside the scope of a law enforcement encounter or use the captured images for purposes other than what is permitted.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Proper supervisory and accountability measures should be in place to make sure individual devices are being used properly.
Limitation of access to footage, revisions, tagging, and other editing tools should be limited to only authorized personnel within the authority chain.
The body worn camera service should log all the single interactions.
The program manager should constantly monitor proper use of the system and enable effective internal audits.
Third-party neutral audits that verify lawful use of the system should be implemented periodically. the bureau should make these audits public.

5.2 Excessive records retention time.

Risk that longer than necessary retention time may allow abuses or enable other risks.

Likelihood: **Unlikely**
Impact: **Moderate**
Risk level: **Low**
Mitigation/Recommendations:

Retention of footage is determined by Oregon Law. The existing law requires a 180-day minimum retention time and a maximum of 30 months for a recording not related to a court proceeding or ongoing criminal investigation.
The bureau needs to make sure that ‘non-evidentiary’ footage is deleted just after the minimum retention schedule.

5.3 Unauthorized sharing of recordings.

Risk of recordings shared with third parties for purposes other than their legal purpose.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Unauthorized sharing of recordings is considered a data breach.

Access to footage needs to be limited to specific tasks like uploading, reporting, reviewing, records management, etc.
Downloading or sharing of footage should be limited to upper management and the records management team.
Proper auditing and accountability measures to correct any harm needs to be in place as part of a response action to the breach.

5.4 Unauthorized Access to video footage.

Risk of unauthorized access, use, disclosure, or removal of audio or video recordings.

Likelihood: **Unlikely**
Impact: **High**
Risk level: **Medium**
Mitigation/Recommendations:

Access to footage needs to be logged by the vendor and limited to specific legal actions or legitimate response to records.
Removal of footage should not be permitted by the vendor's service except in the case of termination of retention time by records management.

6. Financial Impact

6.1 High financial costs of footage storage.

The risk is that, over time, footage will be stored in cloud storage and the cost of maintaining these files and systems may increase the costs of these information technology services, making it a financial burden to the City.

Likelihood: **Possible**
Impact: **Moderate**
Risk level: **Medium**
Mitigation/Recommendations:

Proper estimation of budgetary costs of storing high-definition video footage should be considered.
In some cases, derivative footage from processing for enhancement or records management can create additional costs.
The team may find strategies to save resources and keep in cold storage, or digital storage for low use files, of footage with low evidentiary value.
Additional automatic analysis tools may create additional licensing costs but save staff time for manual editing and revisions.

6.2 Unexpected costs due to training from public complaints may occur.

Additional cost may appear due to unplanned training due to adjustments on the use of equipment or specific aspects of their operations.

Likelihood: **Unlikely**

Impact: **Moderate**

Risk level: **Low**

Mitigation/Recommendations:

Keep clear metrics to identify better ways to use these devices. Officers and supervisors may have recommendations and that creates a more engaging environment.

Essential aspects like initial reporting, analysis, equipment maintenance, automatic and manual operations, etc. may allow officers to feel more confident in the effectiveness of this equipment and systems.

Appendix A
Privacy risk assessment framework

Severity (Evaluate for the worst / highest possible impact)				
	A: Low	**B: Moderate**	**C: High**	**D: Extreme**
Individual Privacy Harms	Customer or "telephone book" information collected and could be disclosed.	Potential disclosure would be limited to non-financial, non-health related information; no personal identifiers (e.g., social security and driver's license #s)	Financial or other highly sensitive information would be collected and disclosable requiring action to remediate negative effects (example: non-HIPAA health data); i.e., credit report management required	Disclosure would result in extreme privacy impacts to highly regulated information; catastrophic public release of financial and personal information requiring credit report monitoring and other remediation
Equity, Disparate Community Impact	Little or no equity impact, technology delivered uniformly without reference to individuals or demographic groups	Accidental or perceived disparate impact to communities by nature of location of technology or service delivered	Intentional disparate equity impact resulting in community concern resulting in privacy harms, media coverage; loss of reputation, legitimacy and trust impacted	Extreme impacts to community, City experiences national media attention; widespread public concern and protest; significant breakdown in business processes associated with damage control
Political, Reputation & Image	Issues could be resolved internally by day-to-day processes; little or no outside stakeholder interest.	Issues could be raised by media and activist community resulting in protests and direct community complaints	Disclosure would likely result in heavy local media coverage; reputation, legitimacy and trust impacted	Likely national and international media coverage; serious public outcry; significant breakdown in business processes associated with mitigation and damage control
City Business, Quality & Infrastructure	Management of disclosure issues would represent negligible business interruption; resolved with no loss of productivity	Issue management would result in brief loss of services; loss of < 1 week service delivery; limited loss of productivity	Significant event; loss of > 1–3-week loss of services; critical service interruption to delivery of infrastructure services	Extreme event; business collapse for department services; loss of > = 3 months of data or productivity; critical business infrastructure loss > 1 month
Legal & Regulatory	Adverse regulatory or legal action not indicated or highly unlikely	Relatively minor incident, regulatory action unlikely; possible legal intervention or consultation for addressing data exposure or loss	Adverse regulatory action likely – i.e., fines and actions associated with CJIS, HIPAA, PCI, NERC, COPPA violations, etc.	Major legislative or regulatory breach; investigation, fines, and prosecution likely; class action or other legal action

Financial Impact	$0-$500 impact; internal costs covered, and no significant external costs incurred	>$500 - $5,000; internal and external costs associated with legal consultation, system rework, overtime	> $5,000 -$50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime	> $50,000 external costs associated with fines, consultation fees and regulatory actions to mitigate information exposure; internal costs associated with system rework, overtime

Likelihood analysis.

For assessing probability of risks

Likelihood	Probability
Almost certain	Likely to occur yearly
Likely	Likely to occur every 2 years
Possible	Likely to occur every 5 years
Unlikely	Likely to occur every 10-20 years
Rare	Has never occurred

Risk Matrix

	Low	**Moderate**	**High**	**Extreme**
Almost Certain				**High**
Likely				
Possible		**Medium**		
Unlikely				
Rare	**Low**			

Appendix B
Definitions

Automated Decision System	A process, set of rules, or tool based on automated processing of data to perform calculations, create new data, or to undertake complex reasoning tasks. This includes advanced methods like artificial intelligence and machine learning, visual perception, speech or facial recognition, and automated translation between languages.
Data	Statistical, factual, quantitative, or qualitative information, in digital or analog form, that is regularly maintained or created by or on behalf of a City bureau and is in a form that can be transmitted or processed.
Data Governance	Definition of policies, processes, and framework of accountability to appropriately manage data as a strategic asset.
Digital Age	This current era whereby social, economic, and political activities are dependent on information and communication technologies. It is also known as the Information Age or the Digital Era.
Information	Information is the result of Data being processed, organized, structured, or presented, allowing it to be used and understood.
Information Protection	A system of Data processing practices related to personally identifiable or identifying Data for the protection of privacy. This includes the management of individual pieces of personal Information, securing Data against unauthorized access, corruption, or loss.
Metadata	A set of Data that describes and gives information about other Data, including its description, origination, and accuracy.
Open Data	Data that can be freely accessed, used, reused, and redistributed by anyone.
Personal Information	Information about a natural person that is readily identifiable to that specific individual. “personal information,” which include, but are not limited to: • identifiers such as a real name, alias, postal address, unique personal identifier, online identifier IP address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers; • payment card industry such as bank account numbers or access codes; • personal health data, such as health history, symptoms of a disease, current health care information, medical device identifiers and serial numbers; • commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies; • biometric information; • internet or other electronic network activity information, that includes browsing history, search history, and information regarding a consumer’s interaction with an Internet Web site, application, or advertisement; • geolocation data, vehicle identifiers (including serial numbers and license plate numbers); • audio, electronic, visual, thermal, olfactory, or similar information; • professional or employment related information; • education information, provided that it is not publicly available; and • inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes
HRAR 11.04 Protection of Restricted and Confidential Information	

Privacy	The ability of an individual to be left alone, out of public view, and in control of information about oneself.
Confidential	Information that is made confidential or privileged by law or the disclosure of information that is otherwise prohibited by law or City policy.
Restricted	Some restrictions or limitations on the use of or disclosure of the information.
Principle of proportionality	The principle of proportionality requires that the processing of personal information must be relevant to, and must not exceed, the declared purpose
Surveillance Technologies	technologies that observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity, or social justice.
Privacy terms	
Effectiveness	This refers to how a specific technology or solution fulfills the pursued objective.
Proportionality	Proportionality is a privacy principle that personal data collected and processed should be adequate, relevant, and limited to that necessary for purpose processed. Proportionality has multiple dimensions. Data collected and used should be adequate, because collecting too little information may lead to incorrect or incomplete information on a data subject. It should also be relevant and limited to what is necessary in relation to the purposes for which it is collected and processed ('data minimization'), both in terms of scope and time (data retention). The proportionality principles consideration of the amount of data to be collected. If excessive data is collected in relation to purposes, then it is disproportionate. Examples: Using biometric data like fingerprints to identify individuals when identity cards would suffice.
data protection	Data protection is the process of protecting data and involves the relationship between the collection and dissemination of data and technology, the public perception and expectation of privacy and the political and legal underpinnings surrounding that data. It aims to strike a balance between individual privacy rights while still allowing data to be used for business purposes. Data protection is also known as data privacy or information privacy. Data protection should always be applied to all forms of data, whether it be personal or enterprise. It deals with both the integrity of the data, protection from corruption or errors, and privacy of data, it being accessible to only those that have access privilege to it.
Frequency of the collection	Periodicity of the data collection.
Privacy safeguards	Measures designed to improve privacy and information protection. It can be represented as below, as, or greater than industry standard and best practices
privacy fundamental rights	Privacy fundamental rights are set to help individuals in being assured of the protection and privacy of their personal data. The General Data Protection Regulation contains a set of 8 privacy fundamental rights. These rights are not legally binding in the US.
Right to information	This right provides the individual with the ability to ask for information about what personal data is being processed and the rationale for such processing. For example, a customer may ask for the list of processors with whom personal data is shared.

Right to access	This right provides the individual with the ability to get access to personal data that is being processed. This request provides the right for individuals to see or view their own personal data, as well as to request copies of the personal data.
Right to rectification	This right provides the individual with the ability to ask for modifications to personal data in case the individual believes that it is not up to date or accurate.
Right to withdraw consent	This right provides the individual with the ability to withdraw a previously given consent for processing of personal data for a purpose. The request would then require stopping the processing of personal data that was based on the consent provided earlier.
Right to object	This right provides the individual with the ability to object to the processing of their personal data. Normally, this would be the same as the right to withdraw consent if consent was appropriately requested and no processing other than legitimate purposes is being conducted. However, a specific scenario would be when a customer asks that their personal data should not be processed for certain purposes while a legal dispute is ongoing in court.
Right to object to automated processing	This right provides the individual with the ability to object to a decision based on automated processing. Using this right, a customer may ask for this request (for instance, a loan request) to be reviewed manually, because of the believe that automated processing of the loan may not consider the unique situation of the customer.
Right to be forgotten	Also known as right to erasure, this right provides the individual with the ability to ask for the deletion of their data. This will generally apply to situations where a customer relationship has ended. It is important to note that this is not an absolute right and depends on your retention schedule and retention period in line with other applicable laws.
Right for data portability	This right provides the individual with the ability to ask for transfer of his or her personal data. As part of such request, the individual may ask for their personal data to be provided back or transferred to another controller. When doing so, the personal data must be provided or transferred in a machine-readable electronic format.

Privacy risk	The term "privacy risk" means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to: 1. Direct or indirect financial loss or economic harm; 2. Physical harm; 3. Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma; 4. Significant inconvenience or expenditure of time; 5. Adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits, or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services; 6. Stigmatization or reputational harm; 7. Disruption and intrusion from unwanted commercial communications or contacts; 8. Price discrimination; 9. Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly: A. Alters that individual's experiences; B. Limits that individual's choices; C. Influences that individual's responses; or D. Predetermines results; or 10. Other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used. 11. Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.
Risk of individual privacy harms	The likelihood that individuals will experience harm or problems resulting from personal data collection and processing
Risk of equity, disparate community impact	The likelihood that specific groups will experience harm or problems resulting from the collection of multiple sources of personal data and their processing.
Risk of political, reputation & image issues	The likelihood that collection or processing of private data may result in harm on professional or personal relationships, harm in reputation or image.
Risk of city business, quality & infrastructure issues	The likelihood that the collection or processing of private data may impact or expose city relationships, agreements, or any other contract, or the quality of those businesses, or built infrastructure
Risk of legal & regulatory issues	The likelihood of any violation of existing laws or regulations by the collection or processing of private information
Risk of financial Impact	The likelihood that ongoing costs in management, collection or processing of private data may become financially inviable or present costs that may not be considered