POWERFUL TECHNOLOGY SOLUTIONS
FOR THE CITY AND PUBLIC WE SERVE

2018 Privacy Impact Assessment

AXON CAPTURE APP

SEATTLE POLICE DEPARTMENT

07.08.2018

Seattle
Information Technology

CONTENTS

PRIVACY IMPACT ASSESSMENT OVERVIEW

WHAT IS A PRIVACY IMPACT ASSESSMENT?

A Privacy Impact Assessment ("PIA") is a method for collecting and documenting detailed information collected in order to conduct an in-depth privacy review of a program or project. It asks questions about the collection, use, sharing, security and access controls for data that is gathered using a technology or program. It also requests information about policies, training and documentation that govern use of the technology. The PIA responses are used to determine privacy risks associated with a project and mitigations that may reduce some or all of those risks. In the interests of transparency about data collection and management, the City of Seattle has committed to publishing all PIAs on an outward facing website for public access.

WHEN IS A PRIVACY IMPACT ASSESSMENT REQUIRED?

A PIA may be required in two circumstances.

- The first is when a project, technology, or other review has been flagged as having a high privacy risk.
- The second is when a technology is required to complete the Surveillance Impact Report process. This is one deliverable that comprises the report.

HOW TO COMPLETE THIS DOCUMENT?

As department staff complete the document, they should keep the following in mind.

- Responses to questions should be in the text or check boxes only, all other information (questions, descriptions, etc.) should **NOT** be edited by the department staff completing this document.
- All content in this report will be available externally to the public. With this in mind, avoid using acronyms, slang, or other terms which may not be well-known to external audiences. Additionally, responses should be written using principally non-technical language to ensure they are accessible to audiences unfamiliar with the topic.

1.0 ABSTRACT

1.1 Please provide a brief description (one paragraph) of the purpose and proposed use of the project/technology.

This 1-3 sentence explanation should include the name of the project/ technology/ program/ application/ pilot (hereinafter referred to as "project/technology"). It should also include a brief description of the project/technology and its function.

Axon Capture is a cell phone application that will allow officers to upload audio and photographs from the phone digital camera and digital audio recorder to www.evidence.com. This application, which SPD plans to pilot by Fall 2018, replaces audio recording devices and standalone cameras to collect evidence and witness statements in the field and allows officers to securely upload that evidence into www.evidence.com immediately, rather than waiting until a later time. The app introduces no new functionality to the process of collecting audio and video evidence; it simply replaces the devices utilized to do so.

1.2 Explain the reason the project/technology is being created or updated and why the PIA is required.

This 1-3 sentence explanation should include the reasons that caused the project/technology to be identified as "privacy sensitive" in the Privacy Threshold Analysis form, such as the project/technology collection of personal information, or that the project/technology meets the criteria for surveillance.

In the course of an investigation, officers collect information as evidence. This may include witness statements and pictures of events (i.e., crime scenes) and/or individuals. Officers currently use digital cameras and audio recording devices to do this. Axon Capture allows officers to gather this information from Department-issued cell phones and immediately upload it to www.evidence.com while on-scene. Concerns about use of the data collected in the course of investigation, while conducted under notice, consent or warrant, may appear to intrude on personal privacy. This review is intended to provide information about the use policies and data management collection practices of this application.

2.0 PROJECT / TECHNOLOGY OVERVIEW

Provide an overview of the project or technology. The overview gives the context and background necessary to understand the purpose, mission and justification for the project / technology proposed

2.1 Describe the benefits of the project/technology.

As opposed to current processes, which require officers to transfer visual and audio evidence to the Department's Digital Evidence Management System (DEMS), Axon Capture allows visual and audio evidence to be collected on scene and uploaded immediately to www.evidence.com to secure the integrity of evidence collection and retention. This reduces any time lag and potential for data loss or corruption between the time of data collection and upload to the evidence collection site.

2.2 Provide any data or research demonstrating anticipated benefits.

The following is a brief case study of cost savings associated with Axon Capture use involving the Redmond, WA Police Department. SPD anticipates similar reduction in time and expense to gather and log photographic evidence.

https://axon.cdn.prismic.io/axon%2F44cb26d0-60c3-4aaf-a4c2-419e85bdb873_case+study+-+axon+capture+-+redmond+pd.pdf

2.3 Describe the technology involved.

Axon Capture is a cell phone application that will allow officers to upload audio, video, and photographs from Department-issued cell phones to www.evidence.com. The application will reside on SPD issued mobile phones.

2.3 Describe how the project or use of technology relates to the department's mission.

Axon Capture helps SPD to efficiently and effectively meet its mission of preventing crime, enforcing the law, and supporting quality public safety by improving the collection and storage of information required in the course of conducting criminal investigations and reducing the time it takes officers to record visual and audio content and upload it.

2.6 Who will be involved with the deployment and use of the project / technology?

All SPD officers will have access to utilize the Axon Capture application in the collection of evidence. Law and policies surrounding the collection and submission of photographic, video, and audio evidence are listed in sections 3.1, 3.3, 4.7, and 5.3 of this document.

3.0 USE GOVERNANCE

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities are bound by restrictions specified in the Surveillance Ordinance and Privacy Principles and must provide written procedures for how the entity will comply with any restrictions identified.

3.1 Describe the processes that are required prior to each use, or access to/ of the project / technology, such as a notification, or check-in, check-out of equipment.

When capturing audio (including video with audio), officers comply with the law, including consent or search warrant requirements of the Washington Privacy Act(Chapt.9.73 RCW). Additionally, SPD Policy 7.110 governs the collection of recorded statements, and requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording. SPD Policy 7.090 governs the handling of photographic evidence.

SPD is in the process of revising current policy to reflect protocols for using Axon Capture including policy directing employees to make reasonable efforts to avoid inadvertently capturing images and video recordings of identifiable individuals or inadvertently capturing conversations and utterances unrelated to specific investigations. The policy will be finalized after the pilot is complete, in order to ensure that it fully addresses privacy and other concerns as well as reflect the officers' functions in the field.

SPD maintains records of all SPD personnel that have been issued City-owned phones.

3.2 List the legal standards or conditions, if any, that must be met before the project / technology is used.

For example, the purposes of a criminal investigation are supported by reasonable suspicion.

Except in limited circumstances, Washington law and SPD policy require officers to notify recorded persons that they are being recorded. (RCW 9.73.030(3), SPD Policy 7.110). RCW 9.73.090(1)(b) and SPD Policy 7.110 impose requirements when taking a recorded statement: officers must state their name, the fact that they are “of the Seattle Police Department”, offense number, date and time of recording, name of interviewee, and all persons present during the interview. The officer must ask the person recorded to respond to the question “Are you aware you are being recorded?” Additionally, officers must give persons in custody Miranda warnings on the recording and ask if victims, witnesses, and complainants if they would like their personal information disclosed or not.

Photographic evidence is collected in accordance with the Intelligence Ordinance (SMC Chapter 14.12) and SPD Policy 6.060.Such evidence must be collected in a way that it does not reasonably infringe upon “individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy.”

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

3.3 Describe the policies and training required of all personnel operating the project / technology, and who has access to ensure compliance with use and management policies.
Include links to all policies referenced.

All officers are trained in the use of the application by other trained officers and unit supervisors. Unit supervisors are responsible for ensuring that all staff receive adequate training.

SPD Policy 7.110 governs the collection of recorded statements (see 3.12 above). SPD Policy 7.090 governs the handling of photographic evidence. SPD Policy 12.040 governs employee use of department-owned computers, devices, and software.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

Additionally, SPD is in the process of revising current policy to reflect protocols for using Axon Capture including policy directing employees to make reasonable efforts to avoid inadvertently capturing images and video recordings of identifiable individuals or inadvertently capturing conversations and utterances unrelated to specific investigations. The policy will be finalized after the pilot is complete, in order to ensure that it fully addresses privacy and other concerns as well as reflect the officers' functions in the field. The policy will include a workflow for officers to follow when they upload photos including the process for "tagging" photos to relate them to a particular incident. This workflow will help ensure that photos are properly indexed so they may be located for cases, public disclosure requests, subpoenas, etc. It is also essential to make sure that photos are properly categorized so the correct retention periods are applied.

4.0 DATA COLLECTION AND USE

Provide information about the policies and practices around the collection and use of the data collected.

4.1 Provide details about what information is being collected from sources other than an individual, including other it systems, systems of record, commercial data aggregators, publicly available data and/or other city departments.

Axon Capture is a component of SPD's Axon Body Worn Camera System, which includes Evidence.Com; however, Axon Capture automatically tags photos and videos with GPS locations from the Department-issued cell phone and metadata is synced to the officer's Evidence.Com user profile.

4.2 What measures are in place to minimize inadvertent or improper collection of data?

As mentioned above, SPD Policy 6.060 requires that officers, when collecting evidence, "gather and record in a manner that does not unreasonably infringe upon: individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience; the exercise of religion; the right to petition government for redress of grievances; and the right to privacy. Consistent with this policy, Department personnel shall comply with the dictates of the Investigations Ordinances and with the requirements of Department rules and regulations."

Additionally, SPD is in the process of revising current policy to reflect protocols for using Axon Capture including policy directing employees to make reasonable efforts to avoid inadvertently capturing images and video recordings of identifiable individuals or inadvertently capturing conversations and utterances unrelated to specific investigations. More details about this policy are outlined in sections 3.1 and 3.3 above.

4.3 How and when will the project / technology be deployed or used? By whom? Who will determine when the project / technology is deployed and used?

Pending leadership approval, SPD intends to pilot the Axon Capture app by Fall 2018.

Following the pilot, the Axon Capture app will be made available on all department phones and accessible to officers whenever a situation warrants the collection of evidence. Law and policy govern the deployment and use of the Axon Capture to collect evidence, as outlined in sections 3.1, 3.3, 4.7, and 5.3 of this document.

4.4 How often will the technology be in operation?

As necessary. The Axon Capture app will be on all SPD mobile phones and accessible to officers whenever a situation or incident includes visual or audio evidence related to an investigation.

4.5 What is the permanence of the installation? Is it installed permanently or temporarily?

The application is a permanent installation on all SPD mobile phones, however, should SPD discontinue its use in the future, the software would be deleted from the mobile phones.

4.6 Is a physical object collecting data or images, visible to the public? What are the markings to indicate that it is in use? What signage is used to determine department ownership and contact information?

Axon Capture is installed on SPD mobile phones. The app is not a physical object that is visible to the public, so no signage is visible. The Department-issued cell phone is visible to the public and individuals will be notified as outlined in section 3.3 of this document. The fact that an officer is taking a photo with a cell phone will often be obvious to an individual, and SPD is in the process of revising current policy to reflect protocols for using Axon Capture including policy directing employees to make reasonable efforts to avoid inadvertently capturing images and video recordings of identifiable individuals or inadvertently capturing conversations and utterances unrelated to specific investigations.

4.7 How will data that is collected be accessed and by whom?

Please do not include staff names; roles or functions only.

Only authorized SPD users can access Axon Capture or the data. Access to the application is limited to SPD personnel via password-protected login credentials.

Data removed from the Axon Capture application is stored on www.evidence.com - securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

All SPD employees are backgrounded and access is controlled by SPD Manual Title 12 provisions governing Department Information Systems including SPD Policy 12.040 - Department-Owned Computers, Devices & Software, SPD Policy 12.050 - Criminal Justice Information Systems, SPD Policy 12.080 – Department Records Access, Inspection & Dissemination, SPD Policy 12.110 – Use of Department E-mail & Internet Systems, and SPD Policy 12.111 – Use of Cloud Storage Services.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols. Please link memorandums of agreement, contracts, etc. that are applicable.

SPD Officers alone operate and use the Axon Capture application on their City-issued mobile phones.

4.9 What are acceptable reasons for access to the equipment and/or data collected?

Officers/Detectives will have access to the equipment in the course of responding to and investigating incidents. The data collected will be accessed for a variety of purposes: Criminal investigations, supervisory review, use of force complaint and internal investigations, training purposes, criminal prosecution and defense, and public disclosure.

4.10 What safeguards are in place, for protecting data from unauthorized access (encryption, access control mechanisms, etc.) and to provide an audit trail (viewer logging, modification logging, etc.)?

Evidence collected by the Axon Capture app does not reside on the cell phone. Instead, it is immediately uploaded to www.evidence.com, which is a secure, privacy-approved solution that is protected from unauthorized access. SPD's data is isolated, not commingled with data from other AXON customers (i.e. any other agency or entity using Evidence.com).

The revised policy described in sections 3.1 and 3.3 will also specify officers shall not retain images or recordings on mobile devices once they have been uploaded to Evidence.com.

5.0 DATA STORAGE, RETENTION AND DELETION

5.1 How will data be securely stored?

Axon supports FIPS 140-2, data is encrypted at rest and in transit, data is not shared, meets CJIS standards, and is a front end that ties into www.evidence.com, which is already a security and privacy- approved solution. All SPD data is isolated, meaning that it is not commingled with any other customer data.

5.2 How will the owner allow for departmental and other entities, to audit for compliance with legal deletion requirements?

SPD's Audit, Policy and Research Section (APRS) can conduct an audit of the any and all systems at any time. In addition, the Office of Inspector General and the federal monitor can access all data and audit for compliance at any time.

5.3 What measures will be used to destroy improperly collected data?

SPD policy contains multiple provisions to avoid improperly collecting data. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a General Offense (GO) Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

Additionally, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

All images must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms guaranteed by the Constitution of the United States and the State of Washington, including freedom of speech, press, association, and assembly; liberty of conscience the exercise of religion; the right to petition government for redress of grievances; and the right to privacy." In the event that information is improperly collected, the Intelligence Ordinance, SMC 14.12, contains purge requirements for information defined as "restricted information" that may be collected in certain circumstances.

All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), and any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

5.4 Which specific departmental unit or individual is responsible for ensuring compliance with data retention requirements?

Unit supervisors are responsible for ensuring compliance with data retention requirements within SPD. Audit, Policy & Research Section personnel can also conduct audits of all data collection software and systems. Additionally, any appropriate auditor, including the Office of Inspector General and the federal monitor can audit for compliance at any time.

6.0 DATA SHARING AND ACCURACY

6.1 Which entity or entities inside and external to the City will be data sharing partners?

SPD has no data sharing partners for Axon Capture. No person, outside of SPD, has direct access to the application or the data.

Data obtained from the system may be shared outside SPD with other agencies, entities, or individuals within legal guidelines or as required by law.

Data may be shared with outside entities in connection with criminal prosecutions:

- Seattle City Attorney's Office
- King County Prosecuting Attorney's Office
- King County Department of Public Defense
- Private Defense Attorneys
- Seattle Municipal Court
- King County Superior Court
- Similar entities where prosecution is in Federal or other State jurisdictions

Data may be made available to requesters pursuant to the Washington Public Records Act, Chapter 42.56 RCW ("PRA"). SPD will apply applicable exemptions to the data before disclosing to a requester. Individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

Per SPD Policy 12.080, the Crime Records Unit is responsible for receiving, recording, and responding to requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies."

Discrete pieces of data collected by audio recording devices may be shared with other law enforcement agencies in wanted bulletins, and in connection with law enforcement investigations jointly conducted with those agencies, or in response to requests from law enforcement agencies investigating criminal activity as governed by SPD Policy 12.050 and 12.110. All requests for data from Federal Immigration and Customs Enforcement (ICE) authorities are referred to the Mayor's Office Legal Counsel in accordance with the Mayoral Directive, dated February 6, 2018.

SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provided by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files collected by the devices.

6.2 Why is data sharing necessary?

Data sharing is necessary for SPD to fulfill its mission of contributing to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of investigation, and to comply with legal requirements.

6.3 Are there any restrictions on non-City data use?

Yes ☒ No ☐

6.3.1 If you answered Yes, provide a copy of the department's procedures and policies for ensuring compliance with these restrictions.

Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20, regulating criminal justice information systems. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260 (auditing and dissemination of criminal history record information systems), and RCW Chapter 10.97 (Washington State Criminal Records Privacy Act).

Once disclosed in response to PRA request, there are no restrictions on non-City data use; however, applicable exemptions will be applied prior to disclosure to any requestor who is not authorized to receive exempt content.

6.4 How does the project/technology review and approve information sharing agreements, memorandums of understanding, new uses of the information, new access to the system by organizations within City of Seattle and outside agencies? Please describe the process for reviewing and updating data sharing agreements.

Research agreements must meet the standards reflected in SPD Policy 12.055. Law enforcement agencies receiving criminal history information are subject to the requirements of 28 CFR Part 20. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

6.5 Explain how the project/technology checks the accuracy of the information collected. If accuracy is not checked, please explain why.

The Axon Capture app capture sounds and images as they are happening in the moment. The application does not check for accuracy, as it is simply capturing a live exchange of sounds and images. It is not interpreting or otherwise analyzing any data it collects.

6.6 Describe any procedures that allow individuals to access their information and correct inaccurate or erroneous information.

Individuals may request records pursuant to the PRA, and individuals have the right to inspect criminal history record information maintained by the department (RCW 10.97.030, SPD Policy 12.050). Individuals can access their own information by submitting a public disclosure request.

7.0 LEGAL OBLIGATIONS, RISKS AND COMPLIANCE

7.1 What specific legal authorities and/or agreements permit and define the collection of information by the project/technology?

SPD's use of Axon Capture's audio recording feature is governed by multiple legal requirements and policies as outlined in sections 3.1, 3.2, 3.3, 4.2, 4.6, and 5.3 of this document.

7.2 Describe what privacy training is provided to users either generally or specifically relevant to the project/technology.

For example, police department responses may include references to the Seattle Police Manual.

SPD Policy 12.050 mandates that all employees receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training. All SPD employees must adhere to laws, City policy, and Department Policy (SPD Policy 5.001), many of which contain specific privacy requirements. Any employees suspected of being in violation of laws or policy or other misconduct are subject to discipline, as outlined in SPD Policy 5.002.

7.3 Given the specific data elements collected, describe the privacy risks identified and for each risk, explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Please work with the Privacy Team to identify the specific risks and mitigations applicable to this project / technology.

Privacy risks revolve around the possibility of improper collection of sounds and images of members of the general public. As it relates to audio recording, SPD mitigates this risk by deploying them consistent to the stipulations outlined in the Washington Privacy Act, Chapt. 9.73 RCW, and only with notification, consent and/or with authorization of a court-ordered warrant. In addition, a number of SPD policies govern the collection of evidence. SPD Policy 7.010 governs the submission of evidence and requires that all collected evidence be documented in a GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence Unit and associated with a specific GO Number and investigation. And, SPD Policy 7.110 governs the collection and submission of audio recorded statements. It requires that officers state their name, the Department name, the General Offense number, date and time of recording, the name of the interviewee, and all persons present at the beginning of the recording.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel that "any documentation of information concerning a person's sexual preferences or practices, or their political or religious activities must be for a relevant reason and serve a legitimate law enforcement purpose." Additionally, officers must take care "when photographing demonstrations or other lawful political activities. If demonstrators are not acting unlawfully, police can't photograph them."

Further, SPD Policy 5.140 forbids bias-based policing and outlines processes for reporting and documenting any suspected bias-based behavior, as well as accountability measures.

Finally, see section 5.3 for a detailed discussion about procedures related to noncompliance.

7.4 Is there any aspect of the project/technology that might cause concern by giving the appearance to the public of privacy intrusion or misuse of personal information?

Examples might include a push of information out to individuals that is unexpected and appears to be intrusive, or an engagement with a third party to use information derived from the data collected, that is not explained in the initial notification.

The privacy risks outlined in section 7.3 above are mitigated by legal requirements and auditing processes (i.e., maintenance of all requests, copies of consent forms/statements and warrants) that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of Axon Capture.

The largest privacy risk is the un-authorized release of a recording that contained information deemed private or offensive in the RCW. To mitigate this risk, the app falls under the current SPD policies around dissemination of Department data and information reflected in section 6.1.

8.0 MONITORING AND ENFORCEMENT

8.1 Describe how the project/technology maintains a record of any disclosures outside of the department.

The Forensics and Digital Imaging Unit is responsible for providing video and digital evidence to prosecuting agencies when investigations are referred for prosecution determination. That Unit maintains logs of cases referred.

Per SPD Policy 12.080, the Crime Records Unit is responsible to receive and record all requests "for General Offense Reports from other City departments and from other law enforcement agencies, as well as from insurance companies." Any subpoenas and requests for public disclosure are logged by SPD's Legal Unit. Any action taken, and data released subsequently in response to subpoenas is then tracked through a log maintained by the Legal Unit. Public disclosure requests are tracked through the City's GovQA Public Records Response System, and responses to Public Disclosure Requests, including responsive records provided to a requestor, are retained by SPD for two years after the request is completed.

8.2 What auditing measures are in place to safeguard the information, and policies that pertain to them, as well as who has access to the audit data? Explain whether the project/technology conducts self-audits, third party audits or reviews.

SPD's Audit, Policy and Research Section is authorized to conduct audits of all investigative data collection software and systems. In addition, the Office of Inspector General and the federal monitor can conduct audits of the software, and its use, at any time. Audit data is available to the public via Public Records Request.