City of Seattle

2021 Surveillance Impact Report Executive Overview

Audio Recording Systems (“Wires”)

Seattle Police Department

Overview

The Operational Policy statements in this document represent the only allowable uses of the equipment and data collected by this technology.

This Executive Overview documents information about the collection, use, sharing, security and access controls for data that is gathered through SPD's Audio Recording Systems. All information provided here is contained in the body of the full Surveillance Impact Review (SIR) document but is provided in a condensed format for easier access and consideration.

1.0 Technology Description

Audio recording devices are typically known as "wires" and can be concealed on a person or hidden in or on objects within a particular environment. Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on. The recording is stored locally on the device and must be downloaded onto a storage device (i.e., thumb drive, external hard drive) before it can be accessed and transcribed.

These devices have the ability to capture audio, video, or both. The legal and investigatory circumstances under which video is captured are different than those under which audio is captured. Video recording systems are discussed in the SIR entitled "Camera Systems".

2.0 Purpose

The mission of the Seattle Police Department is to prevent crime, enforce the law, and support quality public safety by delivering respectful, professional, and dependable police services.

Audio recording systems contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity. These technologies are used only with proper consent and/or a warrant.

Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, wherein an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued. Per law, probable cause is required to obtain a search warrant. Without this technology, SPD would be unable to interrupt ongoing criminal activity and collect important evidence in some criminal investigations.

3.0 Data Collection and Use

Operational Policy: Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.

Audio recording devices collect conversations and sounds of individuals related to a criminal investigation. The information is extracted onto a thumb drive from the device using locally stored computer application that resides on a computer in the TESU Unit. This application, accessible only to TESU staff, is used solely to extract audio data from a device and stores no data.

All of SPD's audio recording devices are managed and maintained by the Technical and Electronic Support Unit (TESU). Once an Officer/Detective has obtained consent and/or a court order, having established probable cause, to utilize an audio recording device, s/he makes a verbal request to the TESU. TESU staff completes TESU's Request Form that requires a reason for the request, a case number associated with the investigation, and a copy of the consent form and/or court order. Each request is screened by the TESU Supervisor prior to deployment.

TESU detectives then assign the audio recording device to the requesting Officer/Detective.

Each deployment is logged, and all request forms (including consent form and/or court order warrant) are maintained within TESU.

4.0 Data Minimization & Retention

Operational Policy: Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.

Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection. All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

As outlined in 2.5 above, if no data is collected by the device that assists in the pursuit of the criminal investigation or falls within the scope of the consent form and/or court order warrant (as determined by the judge), the device is purged in its entirety and no data is provided to the requesting Officer/Detective for the investigation file.

Per the Washington Secretary of State's Law Enforcement Records Retention Schedule, investigational conversation recordings are retained "for 1 year after transcribed verbatim and verified OR until disposition of pertinent case file, whichever is sooner, then Destroy" (LE06-01-04 Rev. 1).

5.0 Access & Security

Operational Policy: Regarding probable cause, detailed requirements spelled out in RCW 9.73.090(2), (4), and (5), and RCW 9.73.120, .130, and .140.

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.**

Access

Only authorized SPD users can access the audio recording devices or the data while it resides in the devices. Access to the systems/technology is limited to TESU personnel via password-protected login credentials.

Data removed from the system/technology and entered into investigative files is securely input and used on SPD's password-protected network with access limited to authorized detectives and identified supervisory personnel.

Security

Audio recording devices store audio data directly on the device. Access to the equipment and data stored on the device is accessible only to TESU staff. TESU staff extract the data, document the extraction, provide the data to the requesting Officer/Detective, and retain no copies of the data.

6.0 Data Sharing and Accuracy

Operational Policy: 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.

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 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).

Data obtained from the system may be shared outside SPD with the 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

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.

7.0 Equity Concerns

Operational Policy: All use of the audio recording systems must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Audio recording systems are used exclusively during the investigation of crimes and only with consent and/or court-ordered warrant, having established probable cause. There is no distinction in the levels of service SPD provides to the various and diverse neighborhoods, communities, or individuals within the city.