City of Seattle

2023 Surveillance Impact Report Executive Overview

Hostage Negotiation Throw Phone

Seattle Police Department

City of Seattle

Overview

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

This Executive Summary documents information about the collection, use, sharing, security and access controls for data that is gathered through Seattle Police Department's Hostage Negotiation Throw Phone. 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

The hostage negotiation throw phone is a phone in a hardened case that is part of a communications system for use in police hostage/crisis negotiations with subjects. The phone case includes microphones and speakers to enable two-way communication in an overt or covert manner. It also includes hidden cameras to support threat and tactical assessments.

2.0 Purpose

This system is intended to provide a reliable means of communication between a hostage taker or barricaded subject and police hostage negotiators. At times there are no other means of phone communication with the subject in a hostage or barricaded person situation and this system allows for safe and reliable communication from a distance. The system allows the team monitoring and recording of conversations to facilitate the development of negotiation strategies and ensure the safety-related information is relayed.

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. RCW 9.73.030 expressly provides an exception to the "all parties" consent rule for the monitoring, intercepting, and recording of calls involving communications with a hostage holder or barricaded person.

Deployment into a constitutionally protected area requires an authorized entry into the area via warrant or warrant exception to include consent, exigent circumstances, or community caretaking/emergency.

The equipment is stored on the HNT truck and can only be accessed by HNT or SWAT team members. If it is prepared for use or deployed on an incident its use is logged on the HNT after-action report.

Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present.

Delivery of the throw phone is typically pre-negotiated with the subject via hailing or other means. For delivery of the throw phone to the subject it is typically brought to the outside of a door or balcony by SWAT team members and the subject is asked to bring it inside for use. It may also be delivered by a large remotely controlled robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door.

Audio/Video data is saved on the hard drive of the DVR/monitoring system. If fully deployed during an actual incident the recordings are downloaded and submitted into evidence or to detectives.

The phone calls are recorded on the laptop running the CINT commander software. Recordings of calls with hostage takers or barricaded subjects are downloaded and submitted into evidence.

Copies of recordings are also kept in the HNT folder on SPD's network. Access to this folder is restricted to HNT, Crisis Response Team, and SWAT/Special Services commanders. The purpose of these files is for debriefing, assessment, and training.

Evidentiary information is downloaded and uploaded into the evidence storage system or provided directly to investigators.

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. RCW 9.73.030 expressly provides an exception to the "all parties" consent rule for the monitoring, intercepting, and recording of calls involving communications with a hostage holder or barricaded person.

Audio/Video data is saved on the hard drive of the DVR/monitoring system. If fully deployed during an actual incident the recordings are downloaded and submitted into evidence or to detectives.

The phone calls are recorded on the laptop running the CINT commander software. Recordings of calls with hostage takers or barricaded subjects are downloaded and submitted into evidence.

Copies of recordings are also kept in the HNT folder on SPD's network. Access to this folder is restricted to HNT, Crisis Response Team, and SWAT/Special Services commanders. The purpose of these files is for debriefing, assessment, and training.

Evidentiary information is downloaded and uploaded into the evidence storage system or provided directly to investigators.

5.0 Access & Security

Operational Policy: 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

Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present.

The throw phone system video and covert audio recording are stored on the DVR system secured in the HNT truck. Only HNT and SWAT SPD employees have access to the HNT truck.

The data is then securely input and used on SPD's password-protected network with access limited to authorized users.

Copies of recordings are kept in the HNT folder on SPD's network. Access to this folder is restricted to HNT, Crisis Response Team, and SWAT/Special Services commanders.

Security

The throw phone system video and covert audio recording are stored on the DVR system secured in the HNT truck. Only HNT and SWAT SPD employees have access to the HNT Truck.

The data is then securely input and used on SPD's password-protected network with access limited to authorized users.

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.

Audio/Video data is saved on the hard drive of the DVR/monitoring system. If fully deployed during an actual incident the recordings are downloaded and submitted into evidence or to detectives.

The phone calls are recorded on the laptop running the CINT commander software. Recordings of calls with hostage takers or barricaded subjects are downloaded and submitted into evidence.

Copies of recordings are also kept in the HNT folder on SPD's network. Access to this folder is restricted to HNT, Crisis Response Team, and SWAT/Special Services commanders. The purpose of these files is for debriefing, assessment, and training.

Evidentiary information is downloaded and uploaded into the evidence storage system or provided directly to investigators.

6.0 Data Sharing and Accuracy

Operational Policy: SPD shares data with authorized researchers pursuant to properly execute research and confidentiality agreements as provide by SPD Policy 12.055. This sharing may include discrete pieces of data related to specific investigative files analyzed by this application. 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).

No person, outside of SPD, has direct access to the data collected with the hostage negotiation throw phone.

Data collected with the hostage negotiation throw phone 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

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 the data collected with the hostage negotiation throw phone 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 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.

Privacy risks revolve around improper collection of images, video, and audio of members of the general public. As it relates to covert recording, SPD mitigates this risk by deploying them consistent to the stipulations outlined in the Washington Privacy Act, Chapt. 9.73 RCW or with reasonable suspicion of criminal activity in areas where no reasonable expectation of privacy exists.

SMC 14.12 and SPD Policy 6.060 direct all SPD personnel to "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, 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 5.3 for a detailed discussion about procedures related to noncompliance.