City of Seattle

2023 Surveillance Impact Report

Hostage Negotiation Throw Phone

Seattle Police Department

Surveillance Impact Report ("SIR") overview

About the Surveillance Ordinance

The Seattle City Council passed Ordinance 125376, also referred to as the "Surveillance Ordinance," on September 1, 2017. SMC 14.18.020.b.1 charges the City's executive with developing a process to identify surveillance technologies subject to the ordinance. Seattle IT, on behalf of the executive, developed and implemented a process through which a privacy and surveillance review is completed prior to the acquisition of new technologies. This requirement, and the criteria used in the review process, are documented in Seattle IT Policy PR-02, the "Surveillance Policy".

How this Document is Completed

This document is completed by the requesting department staff, support and coordinated by the Seattle Information Technology Department ("Seattle IT"). As Seattle IT and department staff complete the document, they should keep the following in mind.

1. 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.

2. 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.

Surveillance Ordinance Review Process

The following is a high-level outline of the complete SIR review process.

Upcoming for Review	Initial Draft	Open Comment Period	Final Draft	Working Group	Council Review
The technology is upcoming for review, but the department has not begun drafting the surveillance impact report (SIR).	Work on the initial draft of the SIR is currently underway.	The initial draft of the SIR and supporting materials have been released for public review and comment. During this time, one or more public meetings will take place to solicit feedback.	During this stage the SIR, including collection of all public comments related to the specific technology, is being compiled and finalized.	The surveillance advisory working group will review each SIR's final draft and complete a civil liberties and privacy assessment, which will then be included with the SIR and submitted to Council.	City Council will decide on the use of the surveillance technology, by full Council vote.

Privacy Impact Assessment

Purpose

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. A PIA 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.

1. When a project, technology, or other review has been flagged as having a high privacy risk.
2. When a technology is required to complete the surveillance impact report process. This is one deliverable that comprises the report.

1.0 Abstract

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

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.

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

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 and this system allows for safe and reliable communication from a distance. The system allows the SPD team monitoring and recording conversations to facilitate the development of negotiation strategies and ensure the safety-related information is relayed. In addition to the overt communication capabilities, this technology also captures images and audio of identifiable individuals, some of whom are unaware of the recording. Without appropriate safeguards, this raises significant privacy concerns.

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.

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.

2.2 Provide any data or research demonstrating anticipated benefits.

Throw phone systems of this nature are standardized equipment for Hostage/Crisis Negotiation Teams according to the National Council of Negotiation Associations, FBI Crisis Negotiation Unit, National Tactical Officers' Association, and other industry standards.

Approximately 15 years ago, the industry standard for these systems began to include video monitoring capabilities. Such monitoring capabilities were deemed important to be able to assess the demeanor of the subject and whether there were any life-safety factors present such as the injured parties or threats of violence.

2.3 Describe the technology involved.

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.

Over the past 20-plus years SPD's Hostage Negotiation Team has utilized throw phone systems from various manufacturers. In addition to a handset, these systems have included a microphone on the box to enable negotiators to hear what the subject is saying without the subject having to pick up the handset.

In addition to a handset for the subject to utilize as a phone, the current throw phone system also includes an external speaker, a microphone, and pinhole type cameras. The external speaker enables negotiators to hail the subject without the subject having to interact with the case. The subject or other parties can be heard through the system through the microphone either by being directed to speak towards the case or by simply monitoring. The cameras are positioned on multiple sides of the box in order to try to provide a 360-degree view. The video feed is sent to a video monitoring system which is monitored so safety information can be relayed to command and SWAT team members.

The phone portion of the system is run through the CINT Commander software on dedicated laptop computers assigned to HNT. The software is installed locally on those computers

The video and audio monitoring portion of the system is managed by software locally installed on the video monitoring DVR console.

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

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. SPD’s department priorities include the use of best practices that include officer safety guidelines and performance-based accountability to provide progressive and responsive police services to crime victims, witnesses, and all members of the community, and to structure the organization to support the SPD mission and field a well-trained sworn and non-sworn workforce that uses technology, training, equipment, and research strategically and effectively.

The Seattle Police Department’s Hostage Negotiation Team (HNT) serves to enhance public safety by providing the Department with a trained, experienced, equipped, and coordinated team of negotiators. It seeks to resolve incidents involving hostage situations, barricaded subjects, and persons in crisis through the use of coordinated tactics, persuasive communication, and specialized equipment. HNT works with patrol and SWAT to provide the highest levels of de-escalation at critical incidents and mitigate the likelihood of force or violence. HNT also supports incidents by gathering information and making assessments and recommendations to SWAT and incident commanders.

The use of the throw phone system provides communication between a hostage taker or barricaded subject and police hostage negotiators.

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

Seattle Police Department’s Hostage Negotiation Team (HNT) is involved in the deployment of the throw phone system, usually in conjunction with SWAT team deployment.

The term “throw phone” is common vernacular for this technology, but this is largely a misnomer as it is not equipment that can be easily or safely thrown. 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 is capable of delivery by a large robot, but this process is very cumbersome in interior environments. For safety purposes occasionally the phone is tossed through an open window or door.

3.0 Use Governance

Provide an outline of any rules that will govern the use of the project / technology. Please note: non-City entities contracting with the City 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.

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.

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

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.

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.

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.

All HNT members are trained on the use and set up of the system upon appointment to the team and refreshed on its use during in-service training.

Supervisors and commanding officers are responsible for ensuring compliance with policies.

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.

4.0 Data Collection and Use

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.

N/A

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

Training on the equipment includes explanation of the monitoring and recording capabilities and limits the recordings to the RCW exemptions of the other legal standards described 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?

The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present.

4.4 How often will the technology be in operation?

The throw phone system is rarely utilized. Of the 168 incidents that HNT responded to in 2021 the throw phone portion of the system was only prepared for delivery a handful of times but was not deployed.

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

Temporary deployment only.

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?

The throw phone is a physical device in a hardened case connected to a console located with SPD negotiators. The delivered portion of the throw phone does not contain identifying labels or markings.

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

Live-feed video is monitored by HNT or SWAT personnel either from the HNT truck, via a system networked laptop, or through a remote view application in range of the wifi system. All of these viewers have controlled access either by password or by permission having to be granted from the main laptop running the software.

Video recorded on the hard drive system is only accessible by HNT members through the DVR system.

Downloaded video that is submitted as evidence is accessible only to SPD employees with authorized access per the investigative or evidence system standards.

Recordings kept in HNT files are accessible to HNT and Crisis Response Team members as well as SWAT and Special Services commanders.

4.8 If operated or used by another entity on behalf of the City, provide details about access, and applicable protocols.

N/A

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

The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present.

Audio or video information collected may be used for follow-up investigation, administrative reviews, and HNT debriefings, training, and member assessments.

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.)?

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.

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

5.0 Data Storage, Retention and Deletion

5.1 How will data be securely stored?

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.

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

SPD's Audit Unit can conduct an audit of any SPD system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time.

SPD conducts periodic reviews of audit logs and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

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 GO Report. SPD Policy 7.090 specifically governs the collection and submission of photographic evidence. Evidence is submitted to the Evidence.com and associated with a specific GO Number and investigation.

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.

Per the CJIS Security Policy:

"5.8.3 Digital Media Sanitization and Disposal The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

5.8.4 Disposal of Physical Media: Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromise by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel."

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?

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.

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.

6.2 Why is data sharing necessary?

Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process. For example, an investigator may send out a photo or description of a homicide suspect in order to find out if another LE agency knows their identity.

Products developed using this information may be shared with other law enforcement agencies. All products created with the information used in this project will be classified as Law Enforcement Sensitive. Any bulletins will be marked with the following restrictions: LAW ENFORCEMENT SENSITIVE — DO NOT LEAVE PRINTED COPIES UNATTENDED — DISPOSE OF IN SHREDDER ONLY – NOT FOR PUBLIC DISPLAY OR DISTRIBUTION — DO NOT FORWARD OR COPY.

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

Yes ☒ No ☐

6.4 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. In addition, Washington State law enforcement agencies are subject to the provisions of WAC 446-20-260, and RCW Chapter 10.97.

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.

6.5 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?

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.

Following Council approval of the SIR, SPD must seek Council approval for any material change to the purpose or manner in which the [system or technology] may be used.

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

The throw phone system captures sounds and images as they are happening in the moment. It does not check for accuracy, as it is simply capturing a live exchange of images and sounds.

6.7 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?

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.

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.

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

SPD Policy 12.050 mandates that all employees, including HNT and SWAT personnel, receive Security Awareness Training (Level 2), and all employees also receive City Privacy Training.

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.

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.

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?

Inherent in video obtained through covert means is the risk that private information may be obtained about members of the public without their knowledge. This risk and those privacy risks outlined in 7.3 above are mitigated by legal requirements and auditing processes that allow for any auditor, including the Office of Inspector General and the federal monitor, to inspect use and deployment of covert cameras.

8.0 Monitoring and Enforcement

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

The HNT Unit does not disclose information collected by the covert cameras. This information is provided to the requesting Officer/Detective to be included in the requisite investigation file.

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 requests for public disclosure are logged by SPD's Public Disclosure Unit. Any action taken, and data released subsequently, is then tracked through the request log. 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.

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.

Financial Information

Purpose

This section provides a description of the fiscal impact of the surveillance technology, as required by the surveillance ordinance.

1.0 Fiscal Impact

Provide a description of the fiscal impact of the project/technology by answering the questions below.

1.1 Current or potential sources of funding: initial acquisition costs.

Current ☒ potential ☐

Date of initial acquisition	Date of go live	Direct initial acquisition cost	Professional services for acquisition	Other acquisition costs	Initial acquisition funding source
12/2016		$24,218.00			Seattle Police Foundation Grant
11/2021		$1,999.00			SPD Budget

Notes:

1.2 Current or potential sources of funding: on-going operating costs, including maintenance, licensing, personnel, legal/compliance use auditing, data retention and security costs.

Current ☐ potential ☐

Annual maintenance and licensing	Legal/compliance, audit, data retention and other security costs	Department overhead	IT overhead	Annual funding source

Notes:

Respond to question 7.3 here

1.3 Cost savings potential through use of the technology

Respond to question 1.3 here

1.4 Current or potential sources of funding including subsidies or free products offered by vendors or governmental entities

Seattle Police Foundation Grant

Expertise and References

Purpose

The following information is provided to ensure that Council has a group of experts to reference while reviewing the completed surveillance impact report ("SIR"). Any individuals or agencies referenced must be made aware ahead of publication that their information has been included. All materials must be available for Council to access or review, without requiring additional purchase or contract.

1.0 Other Government References

Please list any other government bodies that have implemented this technology and can speak to the implementation of this technology.

Agency, municipality, etc.	Primary contact	Description of current use
FBI Crisis Negotiation Unit		
National Council of Negotiation Associations (NCNA)	Phone: 626-533-3636	

2.0 Academics, Consultants, and Other Experts

Please list any experts in the technology under consideration, or in the technical completion of the service or function the technology is responsible for.

Agency, municipality, etc.	Primary contact	Description of current use

3.0 White Papers or Other Documents

Please list any authoritive publication, report or guide that is relevant to the use of this technology or this type of technology.

Title	Publication	Link
Recommend Negotiation Guidelines	National Council of Negotiation Associations	https://ncna.us/default.aspx?MenuItemID=43&MenuGroup=Public+Home

Racial Equity Toolkit ("RET") and engagement for public comment worksheet

Purpose

Departments submitting a SIR are required to complete an adapted version of the Racial Equity Toolkit ("RET") in order to:

- Provide a framework for the mindful completion of the SIR in a way that is sensitive to the historic exclusion of vulnerable and historically underrepresented communities. Particularly, to inform the public engagement efforts departments will complete as part of the surveillance impact report.
- Highlight and mitigate any impacts on racial equity from the adoption and the use of the technology.
- Highlight and mitigate any disparate impacts on individuals or vulnerable communities.
- Fulfill the public engagement requirements of the surveillance impact report.

Adaptation of the RET for Surveillance Impact Reports

The RET was adapted for the specific use by the Seattle Information Technology Departments' ("Seattle IT") Privacy Team, the Office of Civil Rights ("OCR"), and Change Team members from Seattle IT, Seattle City Light, Seattle Fire Department, Seattle Police Department, and Seattle Department of Transportation.

Racial Equity Toolkit Overview

The vision of the Seattle Race and Social Justice Initiative ("RSJI") is to eliminate racial inequity in the community. To do this requires ending individual racism, institutional racism and structural racism. The RET lays out a process and a set of questions to guide the development, implementation and evaluation of policies, initiatives, programs, and budget issues to address the impacts on racial equity.

1.0 Set Outcomes

1.1. Seattle City Council has defined the following inclusion criteria in the surveillance ordinance, and they serve as important touchstones for the risks departments are being asked to resolve and/or mitigate. Which of the following inclusion criteria apply to this technology?

☐ The technology disparately impacts disadvantaged groups.

☐ There is a high likelihood that personally identifiable information will be shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service.

☒ The technology collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection.

☐ The technology raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice.

1.2 What are the potential impacts on civil liberties through the implementation of this technology? How is the department mitigating these risks?

The potential impacts on civil liberties though the use of this technology is that members of the community could fall under surveillance by the covert use of the hostage negotiation throw phone by SPD. The usage of this equipment is situational, and it is used during events in which the HNT Unit responds to police hostage/crisis negotiations with subjects.

1.3 What are the risks for racial or ethnicity-based bias through each use or deployment of this technology? How is the department mitigating these risks?

Include a description of any issues that may arise such as algorithmic bias or the possibility for ethnic bias to emerge in people and/or system decision-making.

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. 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. The use of this technology does not enhance the risks of racial or ethnicity-based bias.

1.4 Where in the City is the technology used or deployed?

☒ all Seattle neighborhoods

- ☐ Ballard
- ☐ Belltown
- ☐ Beacon Hill
- ☐ Capitol Hill
- ☐ Central District
- ☐ Columbia City
- ☐ Delridge
- ☐ First Hill
- ☐ Georgetown
- ☐ Greenwood / Phinney
- ☐ International District
- ☐ Interbay
- ☐ North
- ☐ Northeast
- ☐ Northwest
- ☐ Madison Park / Madison Valley
- ☐ Magnolia
- ☐ Rainier Beach
- ☐ Ravenna / Laurelhurst
- ☐ South Lake Union / Eastlake
- ☐ Southeast
- ☐ Southwest
- ☐ South Park
- ☐ Wallingford / Fremont
- ☐ West Seattle
- ☒ King county (outside Seattle) (Mutual Aid)
- ☒ Outside King County (Mutual Aid)

If possible, please include any maps or visualizations of historical deployments / use.

If possible, please include any maps or visualizations of historical deployments / use here.

1.5 What are the racial demographics of those living in this area or impacted by these issues?

City of Seattle demographics: White - 69.5%; Black or African American - 7.9%; Amer. Indian & Alaska Native - 0.8%; Asian - 13.8%; Native Hawaiian & Pacific Islander - 0.4; Other race - 2.4%; Two or more races - 5.1%; Hispanic or Latino ethnicity (of any race): 6.6%; Persons of color: 33.7%.

King County demographics: White – 70.1%; Black or African American – 6.7%; American Indian & Alaskan Native – 1.1%; Asian, Native Hawaiian, Pacific Islander – 17.2%; Hispanic or Latino (of any race) – 9.4%

1.6 How does the Department to ensure diverse neighborhoods, communities, or individuals are not specifically targeted through the use or deployment of this technology?

The throw phone system is used exclusively during police hostage/crisis negotiations with subjects. There is no distinction in the levels of service SPD provides to the various and diverse neighborhoods, communities, or individuals within the city.

All uses the throw phone by SPD must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

1.7 How do decisions around data sharing have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

The Aspen Institute on Community Change defines *structural racism* as "…public policies, institutional practices, cultural representations and other norms [which] work in various, often reinforcing ways to perpetuate racial group inequity."[1] Data sharing has the potential to be a contributing factor to structural racism and thus creating a disparate impact on historically targeted communities. Data sharing is frequently necessary during the course of a criminal investigation to follow up on leads and gather information on suspects from outside law enforcement agencies. Cooperation between law enforcement agencies is an essential part of the investigative process.

In an effort to mitigate the possibility of disparate impact on historically targeted communities, SPD has established policies regarding the dissemination of data in connection with criminal prosecutions, Washington Public Records Act (Chapter 42.56 RCW), and other authorized researchers.

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.

1.8 How do decisions around data storage and retention have the potential for disparate impact on historically targeted communities? What is the department doing to mitigate those risks?

Like decisions around data sharing, data storage and retention have similar potential for disparate impact on historically targeted communities. The information obtained through the use of the hostage negotiation throw phone is related only to police hostage/crisis negotiations with subjects and its users are subject to SPD's existing policies prohibiting bias-based policing. 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.

1.9 What are potential unintended consequences (both negative and positive potential impact)? What proactive steps can you can / have you taken to ensure these consequences do not occur.

The most important unintended possible consequence related to the continued utilization of the hostage negotiation throw phone by SPD is the possibility that the civil rights of individuals may be compromised by unlawful surveillance. The usage of this equipment is situational, and it is used during events in which the HNT Unit responds to police hostage/crisis negotiations with subjects.

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.

2.0 Public Outreach

2.1 **Scheduled public meeting(s).**

Meeting 1

Location	Virtual
Date	4.18.2023: 11 - 12

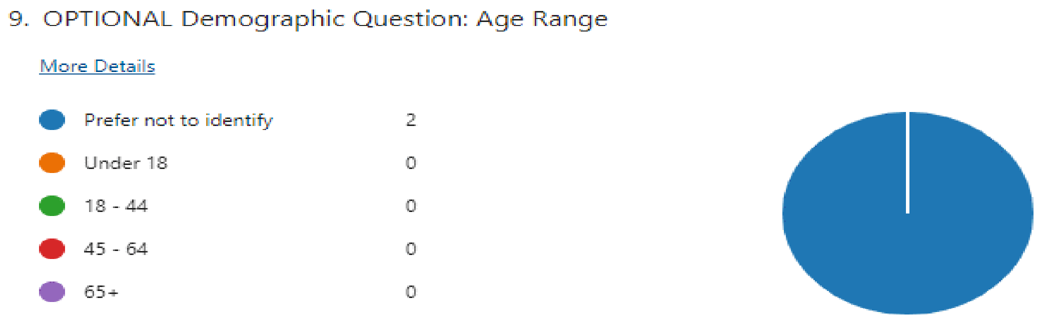
Meeting 2

Location	Virtual
Date	4.28.2023: 11 - 12

3.0 Public Comment Analysis

This section was completed after the public comment period closed on 5.19.2023.

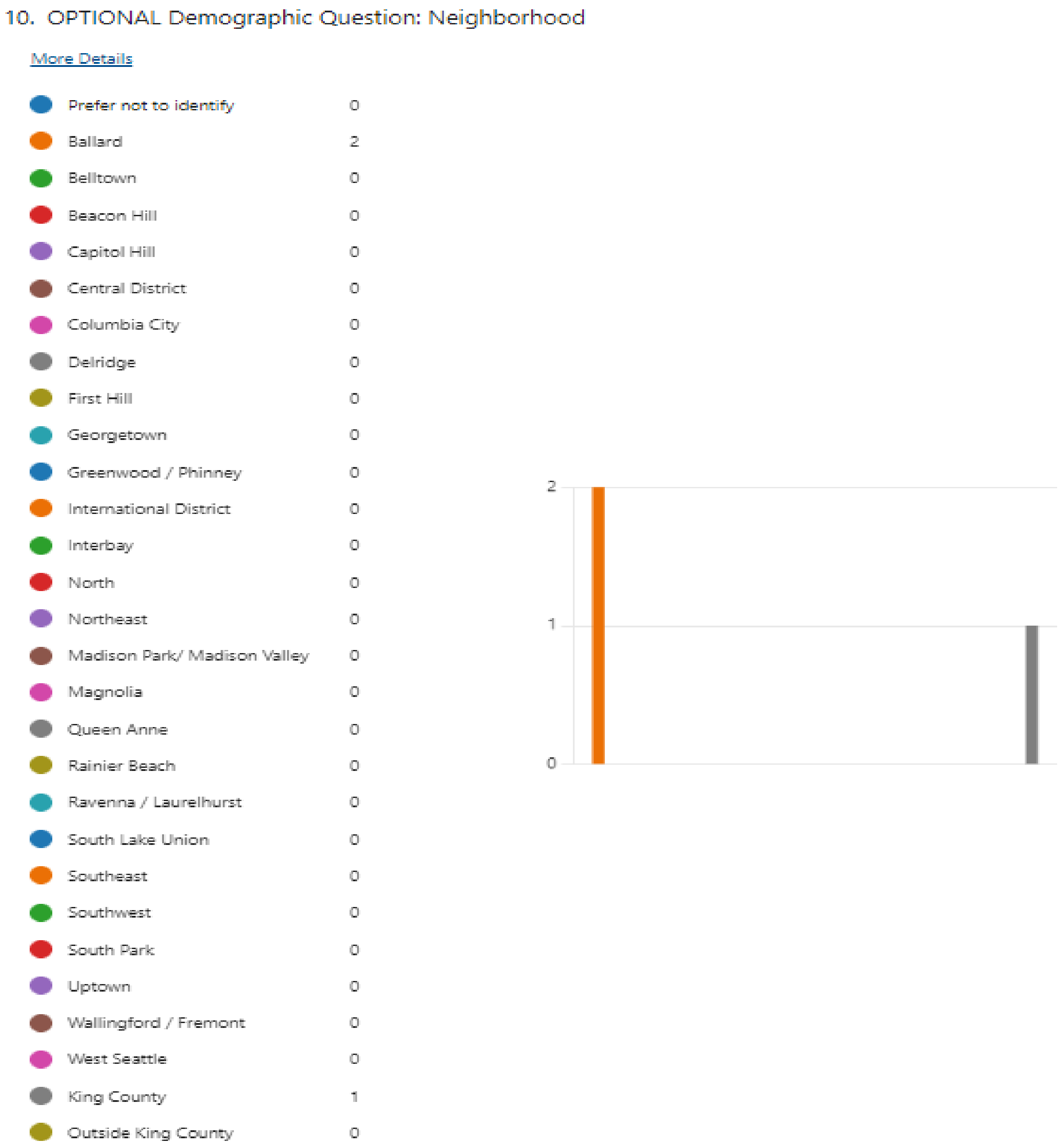
3.1 Summary of Response Demographics



9. OPTIONAL Demographic Question: Age Range

More Details

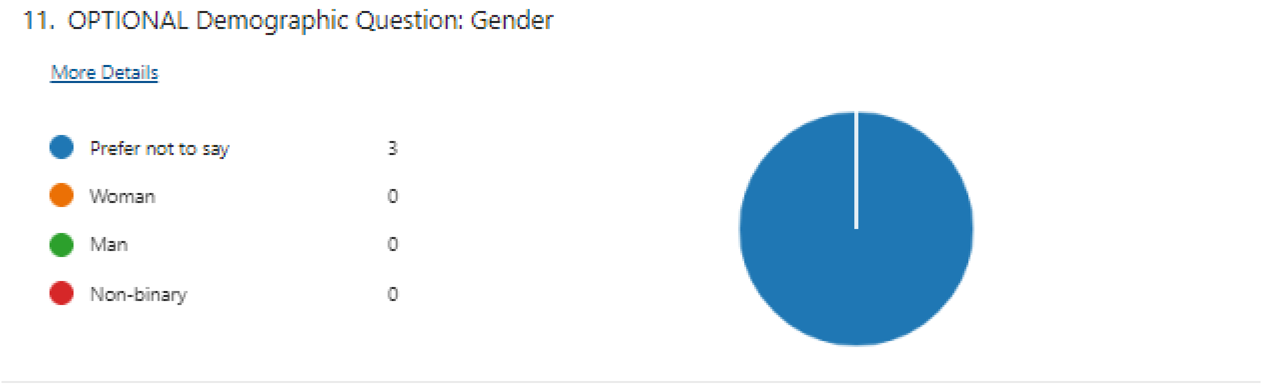
●	Prefer not to identify	2
●	Under 18	0
●	18 - 44	0
●	45 - 64	0
●	65+	0



10. OPTIONAL Demographic Question: Neighborhood

More Details

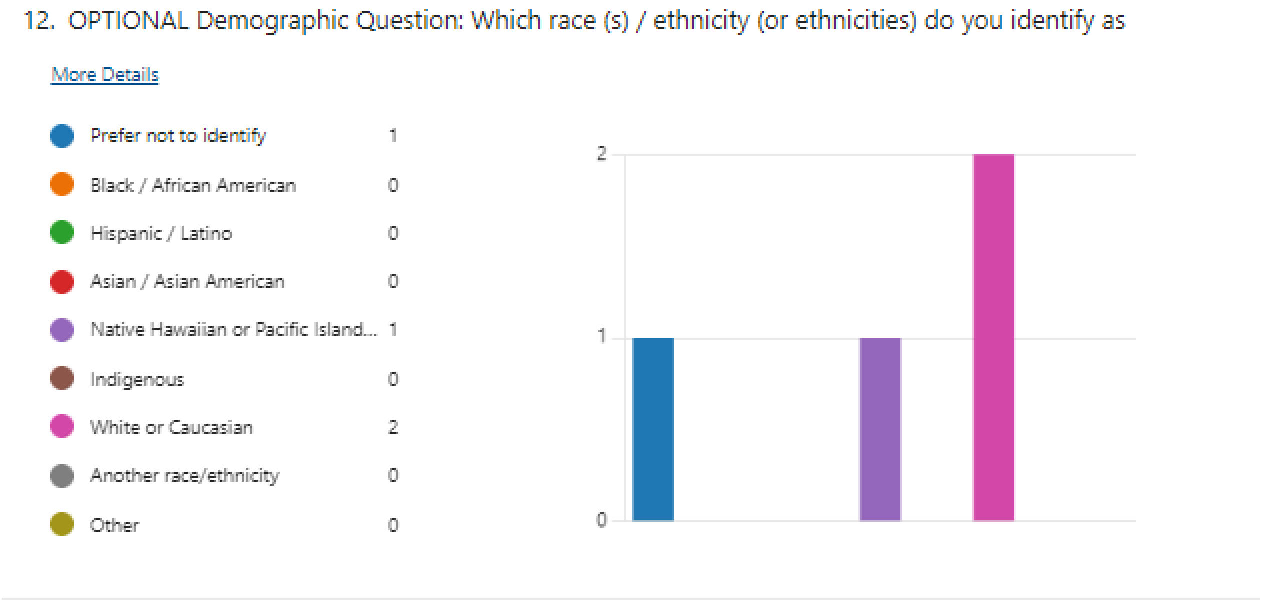
●	Prefer not to identify	0
●	Ballard	2
●	Belltown	0
●	Beacon Hill	0
●	Capitol Hill	0
●	Central District	0
●	Columbia City	0
●	Delridge	0
●	First Hill	0
●	Georgetown	0
●	Greenwood / Phinney	0
●	International District	0
●	Interbay	0
●	North	0
●	Northeast	0
●	Madison Park/ Madison Valley	0
●	Magnolia	0
●	Queen Anne	0
●	Rainier Beach	0
●	Ravenna / Laurelhurst	0
●	South Lake Union	0
●	Southeast	0
●	Southwest	0
●	South Park	0
●	Uptown	0
●	Wallingford / Fremont	0
●	West Seattle	0
●	King County	1
●	Outside King County	0



11. OPTIONAL Demographic Question: Gender

More Details

●	Prefer not to say	3
●	Woman	0
●	Man	0
●	Non-binary	0



12. OPTIONAL Demographic Question: Which race (s) / ethnicity (or ethnicities) do you identify as

More Details

●	Prefer not to identify	1
●	Black / African American	0
●	Hispanic / Latino	0
●	Asian / Asian American	0
●	Native Hawaiian or Pacific Island...	1
●	Indigenous	0
●	White or Caucasian	2
●	Another race/ethnicity	0
●	Other	0

3.2 Question One: What concerns, if any, do you have about the use of this technology?

Respondent 2:

1. Capturing and retaining audio and video of people other than the hostage-taker without proper consent and authorization.

Respondent 3:

2. No SPD policy defining or limiting the (CAD/etc) incident types for which SPD may use the throw phones (such as to only incidents types that map to "hostage holder or barricaded person"), meaning they could be used at a public protest or other unintended locations.

3. Because the CINT Commander software and throw phone have almost no market competition and aren't available to the general public, this makes them ripe for likely having security weaknesses. Examples of some possible security weaknesses here could include: requiring the use of out-of-date operating systems (such as Windows XP or Vista as mentioned in the CINT Commander Manual) thus exposing the laptop to a wide variety of security vulnerabilities; using poor WiFi security (such as WEP or WPA, which can be cracked in minutes); buffer overflow vulnerabilities; default username/password; Man-in-the-Middle vulnerabilities; and/or spoofing an SPD officer (among other possibilities). Additionally, the SIR doesn't mention this technology ever having gone through an internal security review or an external security penetration test. It seems possible that the security of SPD's use of the throw phone is resting on the combination of: low public awareness about the technology + low frequency of deployment + needing to be within WiFi range; but none of those would be considered a security protection or remediation of any vulnerabilities.
4. Overlapping with the lack of an internal security review is also the seeming lack of a threat model for SPD's use of the throw phone. For example, a threat model might find that the transfer of recordings to physical media opens up the risk for said physical media getting lost/stolen and it also introduces risk of lack of oversight regarding whether any copies of the physical media are made, by whom, and where are those media are now located. A typical security review should include some form of a threat model (even if it's only the informal notions of one), which would also include steps to take to mitigate each risk.

5. The retention of recordings on the throw phone video monitoring console's harddrive for an indeterminate likely multi-year retention period (including for recordings that may be sensitive in nature but not deemed of evidentiary value) seems potentially unwise and not well thought out. Shouldn't the retention period be intentional, not an outcome of the harddrive size and amount of device usage?

6. Incomplete information in the SIR. SPD provided very helpful information that clarifies a number of confusing areas of the SIR. SPD's answers to the public should also be accessible inside the SIR, so that anyone in the future reading the SIR has this same clarifying information.

(CONTINUED FROM ABOVE)

6) Nothing prevents SPD from using biometric tools or systems (such as voice, face, or gait analysis) on the live audio-video feed or the recordings. That is, SPD has said that such "tools are not part of the system", but they could start using tools in the future.

7) SPD Policy 7.090 only addresses evidence. There could be recordings from the throw phone that don't show the suspect in-frame and thus aren't evidence but do show a victim perhaps not fully clothed, so that livestream should not be recorded by non-departmental devices. I appreciate that SPD said they plan to create a policy around this; but as it stands today, this is still a concern since there isn't said policy.

8) Questions only submitted in writing (not at the public engagement meeting) have not been answered by SPD (as of at least May 11, 2023).

3.3 Question Two: What value, if any, do you see in the use of this technology?

Respondent 2: Having a secure means of communication in hostage situations.

3.4 Question Three: What would you want City leadership to consider when making a decision about the use of this technology?

Respondent 2:
Are the safeguards to limit the visibility of the data that's been recorded, and ensure deletion of any data of others, sufficient.

Respondent 3: Based on the above concerns, these are my recommendations:

1) City Council should require the SPD Policy to be updated to limit the use of the throw phone(s) to only the incident types that map to "hostage holder or barricaded person".

2) City Council should request an internal security review with a threat model (even a simple one) be done of the throw phone system and the end-to-end workflows in use.

3) City Council should review and potentially revise the current practice of retention of recordings on the throw phone video monitoring console's harddrive for an indeterminate likely multi-year retention period based purely on the size of the harddrive and amount of device usage.

4) City Council should require the SIR to be updated to include the Q&A between the public and SPD. SPD provided very helpful information that clarifies a number of confusing areas of the SIR. SPD's answers to the public should also be accessible inside the SIR, so that anyone in the future reading the SIR has this same clarifying information.

5) City Council should prohibit SPD from using biometric tools or systems (such as voice, face, or gait analysis) on the live audio-video feed or the recordings from the throw phone system.

(Continued from above)

6) City Council should reinforce the need for there to be an SPD policy prohibiting the recording of the livestream screen using a non-departmental device (i.e. personal cellphone) nor taking such recordings for non-official use (even with a departmental device).

7) City Council should require that all of the public's questions are to be answered before the SIR progresses through the rest of the Ordinance's process.

3.5 Question Four: General response to the technology.

Respondent 1:
New questions:
1) Has the throw phone ever been deployed or prepared for deployment at any public protest?
2) Does the video data ever leave SPD-owned equipment? That is, is any portion of the data flow hosted externally (i.e. by 836 Technologies providing livestreamming that is Software-as-a-Service) or is the data always local to the throw phone devices and SPD-owned networked devices?
3) How many throw phones does SPD own?
4) Is 836 Technologies the only manufacturer of throw phones that SPD owns?
5) Is there any section of the SPD Manual that limits deployment of a throw phone to the CAD event/incident type(s) that map to a "hostage holder or barricaded person"?
Questions given at 1st public engagement meeting:
1)Item 2.3 in the SIR mentions a microphone & cameras - Is it always also recording audio & video from all the mics and cameras or does an SPD officer need to turn on recording for each mic or camera?
2)Is the video feed mentioned Item 2.3 in the SIR served over a wired or wireless connection?
3)Who is responsible for deleting the recordings from the throw phone video monitoring console's harddrive after they have been uploaded into evidence; and how long are recordings kept on its harddrive before they are deleted?
4)Is any part of the throw phone system connected to the SPD network? Item 5.2 in the SIR says that the software automatically alerts users of data that must be deleted under legal deletion requirements; however, that seems unlikely for data stored on systems not connected to the network. Are there automated alerts regarding data deletion for data on the throw phone console? If so, who receives those alerts?
5)Item 4.7 in the SIR says that downloaded video is submitted as evidence, but doesn't explain how that recording is transferred there - Are the recordings downloaded onto a USB stick, burned onto a DVD, or is the throw phone's console connected to the SPD network for direct transfer of files?
6)Who decides which recordings will be stored in the HNT folder on the SPD network?
7)Item 5.3 in the SIR asks "What measures will be used to destroy improperly collected data?" and SPD's answer covers data that is evidence; but per item 4.9 in the SIR only 1 out of the 5 reasons for retaining a recording was for evidence in investigations, so what happens with recordings not retained as evidence; and also in 5.3 SPD answered with the CJIS Security Policy on disposal of digital media, but it's unlikely that SPD is throwing the video monitoring system in the garbage after each deployment, so what is the actual data lifecycle and what ensures data not in scope as evidence is promptly deleted?
8)What if any additional sensors are on the throw phone?
9)Who is responsible for keeping the software up-to-date?
10)Has SPD purchased or used any Satellite-based services for their throw phones?
11)Item 5.1 in the SIR says recordings are kept in an HNT folder - Are there access logs for that folder and is there monitoring/alerting for anomalous access to it?
12)Is there any policy on how many & which computers can be connected to the CINT Commander's LAN?
13)Is there any SPD policy regarding how many & which bluetooth devices can be paired with the CINT Commander?
14)Who decides which recordings are kept as evidence?
15)Is there any SPD policy regarding which types of media are allowed to be used for transferring data off of the CINT Commander, such as a USB stick is allowed but not CDs/DVDs?
16)How is the live video feed secured?
17)Does SPD use any biometric tools or systems (such as voice, face, or gait analysis) on the live audio-video feed or the recordings?
18)What policy prohibits SPD employees from using a cellphone to record the live video feed screen?
19)When was the last audit of the throw phone system and where can the public see a copy of that report?

Respondent 2:

How many HNTs does SPD own? What vendors and models are they? Does any information get shared with the vendor? If so what are the contractual arrangements limiting their use of the data?

Section 4.4 only has information about usage in 2021. How many times was a HNT used in earlier years? In 2022?

How does the data get from the DVR system to the rest of the SPD network? [4.10 says it's "securely input" into the network, 5.1 says it's "downloaded and submitted" into evidence and also talks about it keeping it in the HNT folders.]

What are the criteria for the decisions about what data is recorded for evidence and what is stored for administrative, assessment, and followup use?

When deciding whether to keep recordings for evidence (or for use in training and assessment), what considerations are taken into account about information that may have been captured relating to other people besides the hostage taker or barricaded subject?

Under what situations is data recorded by the HNT archived (or kept as a backup)?

Section 5.2 notes that the Audit Unit can conduct an audit at any time. Have any audits been conducted, and if so are the results available publicly?

3.6 General Surveillance Comments These are comments received that are not particular to any technology currently under review.

Respondent 1: FYI, My questions below in section 4 have been heavily reduced due to the character count limit imposed by Seattle IT.

Respondent 3: The silent character count limit on this public comment survey form results in either truncated text and/or an artificial inflation of survey responses. This public comment survey form also results in text disappearing and re-appearing as I scroll, which is a very confusing experience and certainly not accessible. It seems the use of this survey-technology-provider was not well tested.

4.0 Response to Public Comments

This section will be completed after the public comment period has been completed.

4.1 How will you address the concerns that have been identified by the public?

What program, policy and partnership strategies will you implement? What strategies address immediate impacts? Long-term impacts? What strategies address root causes of inequity listed above? How will you partner with stakeholders for long-term positive change?

5.0 Equity Annual Reporting

5.1 What metrics for this technology be reported to the CTO for the annual equity assessments?

Respond here.

Privacy and Civil Liberties Assessment

Purpose

This section shall be completed after public engagement has concluded and the department has completed the racial equity toolkit section above. The privacy and civil liberties assessment is completed by the community surveillance working group ("working group"), per the surveillance ordinance which states that the working group shall:

Working Group Privacy and Civil Liberties Assessment

From: Seattle Community Surveillance Working Group (CSWG)
To: Seattle City Council
Date: July 17, 2023
Re: Privacy and Civil Liberties Impact Assessment for Audio Recording Systems

Executive Summary

The CSWG has completed its review of the Surveillance Impact Report (SIR) for Hostage Negotiation Throw Phones as part of the Seattle Surveillance Ordinance technology review process. This document is the CSWG's Privacy and Civil Liberties Impact Assessment for Hostage Negotiation Throw Phones used by Seattle Police Department (SPD) as set forth in SMC 14.18.080(B)(1), which we provide for inclusion in the final SIRs submitted to the City Councils.

This document first provides our recommendations to Council, then provides background information, key concerns, and outstanding questions regarding Hostage Negotiation Throw Phones.

Our assessment of Hostage Negotiation Throw Phones as used by Seattle Police Department (SPD) focuses on six major issues:

1. It is unclear how many and what specific devices are used by SPD.
2. It is unclear how and how often SPD uses the devices (e.g., in an overt or covert manner).
3. It is unclear if there are limitations on the specific purposes for which SPD may use the devices.
4. It is unclear if there have been security review or audits of the technology.
5. There are inadequate data retention policies.
6. There are no prohibitions on the use of biometric technology on or with the technology.

Recommendations

The Council should adopt clear and enforceable rules that ensure, at the minimum, the following:

1. The purpose and allowable uses of the hostage negotiation throw phone(s) must be narrowly and clearly defined, and any SPD use of this technology must be limited to that specific purpose and those allowable uses. There must be a requirement for SPD to limit the use of throw phone(s) to only the incident types that map to "hostage holder or barricaded person".
2. There must be a requirement for SPD to disclose how and how often the hostage negotiation throw phone(s) are used (e.g., the number of times it is used in a covert manner, without knowledge or consent).
3. There must be an internal or external security review of the technology.
4. There must be a requirement for an independent audit of SPD's hostage negotiation throw phone(s) and that audit must be made publicly available.
5. There must be a review and revision of the retention policy and SPD's practice of retaining recordings on the throw phone video monitoring console's hard drive based solely on the size of the hard drive and the amount of device usage.
6. There must be a prohibition on use of biometric technology on or with hostage negotiation throw phones.

Key Concerns

4. **There is no specific policy defining or limiting the incident types for which SPD may use the throw phones.** For example, there is not a policy stating that the throw phones may only be used for incidents that map to “hostage holder or barricaded person,” leaving open the possibility that the throw phones could be used at a public protest or other unintended locations.
5. **It is unclear how many throw phones SPD owns and what manufacturers make these phone(s).**
6. **It is unclear how and how often the hostage negotiation throw phone(s) are used.** While 2021 statistics are included, statistics from other years are not. While the SIR states that most of the time the throw phones are used with the knowledge and consent of the barricaded person, it does not provide specific details on the number of times the technology is used overtly versus covertly, without the knowledge and consent of those being recorded.
7. **There are inadequate auditing policies and practices.** The SIR does not state whether SPD’s use of the throw phones has ever been audited.
8. **There are inadequate retention policies.** It is unclear what the retention period is for the recordings on the throw phone video monitoring console’s hard drive. The retention period should be limited to what is strictly necessary for the technology’s purpose and should not be driven by the hard drive size and amount of device usage.
9. **There are inadequate security safeguards.** The SIR does not state whether the technology has been subject to an internal security review or an external security penetration test.
10. **There is no prohibition of the use of biometric tools or systems (e.g., voice, face, or gait analysis) on the live audio-video feed or the recordings.**

Outstanding Questions

- Has the throw phone ever been deployed or prepared for deployment at a protest?
- Does the video data ever leave SPD-owned equipment?
- How many throw phones does SPD own and what are the manufacturers?
- Is there any section of the SPD manual that limits deployment of a throw phone to an incident type that maps to a “hostage holder or barricaded person”?
- Who decides which recordings are kept as evidence?
- Has there been an audit of the system and if so, is it publicly available?

The answers to these questions can further inform the content of any binding policy the Council chooses to include in an ordinance on this technology, as recommended above.

City of Seattle

CTO Response to Working Group Assessment

Memo

Date: August 4th, 2023

To: Seattle City Council

From: Jim Loter, Chief Technology Officer, City of Seattle

Subject: CTO Response: Surveillance Working Group Hostage Negotiation Throw Phone SIR Review

Purpose

As provided in the Surveillance Ordinance, SMC 14.18.080, this memo outlines the Chief Technology Officer's (CTO's) response to the Surveillance Working Group assessment on the Surveillance Impact Report for Seattle Police Department, Hostage Negotiation Throw Phone.

Background

The Information Technology Department (ITD) is dedicated to meeting the objectives of the Privacy Principles and Surveillance Ordinance to provide oversight and transparency about the use and acquisition of specialized technologies with potential privacy and civil liberties impacts. All City departments have a shared mission to protect lives and property while balancing technology use and data collection with negative impacts to individuals. This requires ensuring the appropriate use of privacy invasive technologies through technology limitations, policy, training, and departmental oversight.

The CTO's role in the SIR process has been to ensure that all City departments are compliant with the Surveillance Ordinance requirements. As part of the review work for surveillance technologies, ITD's Privacy Office has facilitated the creation of the Surveillance Impact Report documentation, including collecting comments and suggestions from the Working Group and members of the public about these technologies. ITD and City departments have also worked collaboratively with the Working Group to answer additional questions that came up during their review process.

Technology Purpose

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.

Working Group Concerns

In their review, the Working Group has raised concerns about these devices being used in a privacy impacting way, including concerns related to definitive policy governing the use of the technology, inventory and manufacturer information, the frequency which the phones are used, questions around auditing policies and practices, questions related to retention, security safeguards, and the lack of prohibition related to biometric tools and use during live audio-video feed. We believe that policy, training, and technology limitations enacted by SPD provide adequate mitigation for the potential privacy and civil liberties concerns raised by the Working Group about the use of this important operational technology.

Recommended Next Steps

I look forward to working together with Council and City departments to ensure continued transparency about the use of these technologies and finding a mutually agreeable means to use technology to improve City services while protecting the privacy and civil rights of the residents we serve. Specific concerns in the Working Group comments about hostage negotiation throw phones are addressed in the attached document.

Response to Specific Concerns:

Concern: There is no specific policy defining or limiting the incident types for which SPD may use the throw phones.
CTO Assessment: The specific use of this technology is limited to use in police/hostage crisis negotiations as described in the SIR. The SIR Process designates that if the Hostage Negotiation Throw Phone (HNT) ordinance is approved by City Council, the detail in the SIR become the approved uses and protections. Any use outside of what is codified in the SIR - in this case, the use of this technology outside of hostage incidents - would be in violation of the ordinance.
SIR response:
Section 2.3
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.

Section 2.4
The use of the throw phone system provides communication between a hostage taker or barricaded subject and police hostage negotiators.

Section 4.9
The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present.

RET Section 1.4.2
The throw phone system is used exclusively during police hostage/crisis negotiations with subjects. There is no distinction in the levels of service SPD provides to the various and diverse neighborhoods, communities, or individuals within the city.

All uses the throw phone by SPD must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.

Concern: It is unclear how many throw phones SPD owns and what manufacturers make these phone(s).
CTO Assessment: The amount of throw phones and manufacturers are not questions represented in the SIR. Below is information that was included that gives greater context to the frequency of the use of this technology. This question may be part of the OIGs audit of the technology through the surveillance process.

SIR response:

Section 2.3
Over the past 20-plus years SPD's Hostage Negotiation Team has utilized throw phone systems from various manufacturers.

Concern: It is unclear how and how often the hostage negotiation throw phone(s) are used.

CTO Assessment: The use of this technology appears to be rare and based on situational awareness and with the approval and authorization of multiple commanders prior to deployment. This question may be part of the OIGs audit of the technology through the surveillance process.

SIR response:

Section 4.3
The throw phone is used in police hostage/crisis negotiations with subjects often at times when there are no other means of phone communication. Deployment of the throw phone system on an incident involves the authorization of the HNT supervisor, incident commander, and the SWAT commander if present.

Section 4.4
The throw phone system is rarely utilized. Of the 168 incidents that HNT responded to in 2021 the throw phone portion of the system was only prepared for delivery a handful of times but was not deployed.

Concern: There are inadequate auditing policies and practices.

CTO Assessment: Technology audits, including deployment of HNT, may be conducted by the Office of the Inspector General and/or by the Audit Unit within SPD at their discretion. Additionally, ordinance requirements stipulate annual usage reviews of surveillance technologies, including Hostage Negotiation Throw Phones, must be conducted of the OIG.

SIR response:

Section 5.2
SPD's Audit Unit can conduct an audit of any SPD system at any time. In addition, the Office of Inspector General can access all data and audit for compliance at any time.

SPD conducts periodic reviews of audit logs, and they are available for review at any time by the Seattle Intelligence Ordinance Auditor under the City of Seattle Intelligence Ordinance. The software automatically alerts users of data that must be deleted under legal deletion requirements such as 28 CFR Part 23.

Concern: There are inadequate security safeguards.

CTO Assessment: Based on the response to public comment question 15 in the second public comment meeting this is a highly restricted and controlled system. Specifically, SPD describes the following setup associated with HNT:

> *"requires monitor to be hardwired into trucks Lan system. Satellite software to be installed on the satellite computer. Satellite computer must be on the wired or password protected LAN network. And for CINT computer must also allow access. For Mobile device requires viewer software to be installed on the mobile device, the device to be within Wi-Fi range, and for user to use the account name and password." Additionally, "access to HNT folder is limited. Security requirements related to anomalous access managed by ITD) as well as request for access."*

SIR response:

Section 4.10
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.

Section 5.1:
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.

Concern: There is no prohibition of the use of biometric tools or systems (e.g., voice, face, or gait analysis) on the live audio-video feed or the recordings.

CTO Assessment: Based on the response to question 16 in the second public comment meeting, this tool does not use any biometric tools for the live audio/video feed. They are not part of this system.
Additionally, privacy risks are outlined and mitigation described in section 7.3 of the SIR (see below). Additionally, the SIR Process designates that if the Hostage Negotiation Throw Phone (HNT) ordinance is approved by City Council, the detail in the SIR become the approved uses and protections; any use outside of what is codified in the SIR, in this case, the use of biometric tools or systems on live audio or recordings, would be in violation of the ordinance, barring undergoing the material change process and re-submittal to Council.

SIR response: This question is not represented in the SIR. This was answered during public comment (see video). Also noting the technology system capabilities described in SIR:

Section 6.5
The throw phone system captures sounds and images as they are happening in the moment.

Section 7.3
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.

Appendix A: Glossary

Accountable: (taken from the racial equity toolkit.) Responsive to the needs and concerns of those most impacted by the issues you are working on, particularly to communities of color and those historically underrepresented in the civic process.

Community outcomes: (taken from the racial equity toolkit.) The specific result you are seeking to achieve that advances racial equity.

Contracting equity: (taken from the racial equity toolkit.) Efforts to achieve equitable racial outcomes in the way the City spends resources, including goods and services, consultants and contracting.

DON: "department of neighborhoods."

Immigrant and refugee access to services: (taken from the racial equity toolkit.) Government services and resources are easily available and understandable to all Seattle residents, including non-native English speakers. Full and active participation of immigrant and refugee communities exists in Seattle's civic, economic and cultural life.

Inclusive outreach and public engagement: (taken from the racial equity toolkit.) Processes inclusive of people of diverse races, cultures, gender identities, sexual orientations and socio-economic status. Access to information, resources and civic processes so community members can effectively engage in the design and delivery of public services.

Individual racism: (taken from the racial equity toolkit.) Pre-judgment, bias, stereotypes about an individual or group based on race. The impacts of racism on individuals including white people internalizing privilege, and people of color internalizing oppression.

Institutional racism: (taken from the racial equity toolkit.) Organizational programs, policies or procedures that work to the benefit of white people and to the detriment of people of color, usually unintentionally or inadvertently.

OCR: "Office of Civil Rights."

Opportunity areas: (taken from the racial equity toolkit.) One of seven issue areas the City of Seattle is working on in partnership with the community to eliminate racial disparities and create racial equity. They include: education, health, community development, criminal justice, jobs, housing, and the environment.

Racial equity: (taken from the racial equity toolkit.) When social, economic and political opportunities are not predicted based upon a person's race.

Racial inequity: (taken from the racial equity toolkit.) When a person's race can predict their social, economic, and political opportunities and outcomes.

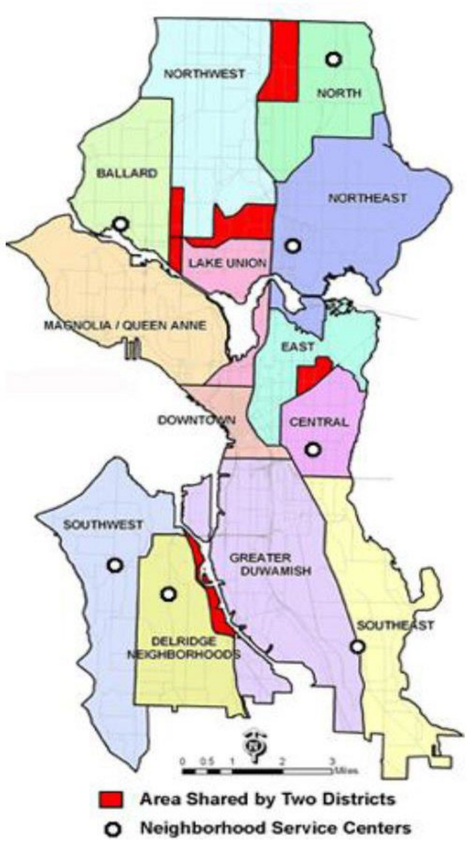
RET: "racial equity toolkit"

Seattle neighborhoods: (taken from the racial equity toolkit neighborhood.) Boundaries defined for the purpose of understanding geographic areas in Seattle.

Stakeholders: (taken from the racial equity toolkit.) Those impacted by proposed policy, program, or budget issue who have potential concerns or issue expertise. Examples might include: specific racial/ethnic groups, other institutions like Seattle housing authority, schools, community-based organizations, change teams, City employees, unions, etc.

Structural racism: (taken from the racial equity toolkit.) The interplay of policies, practices and programs of multiple institutions which leads to adverse outcomes and conditions for communities of color compared to white communities that occurs within the context of racialized historical and cultural conditions.

Surveillance ordinance: Seattle City Council passed ordinance 125376, also referred to as the "surveillance ordinance."



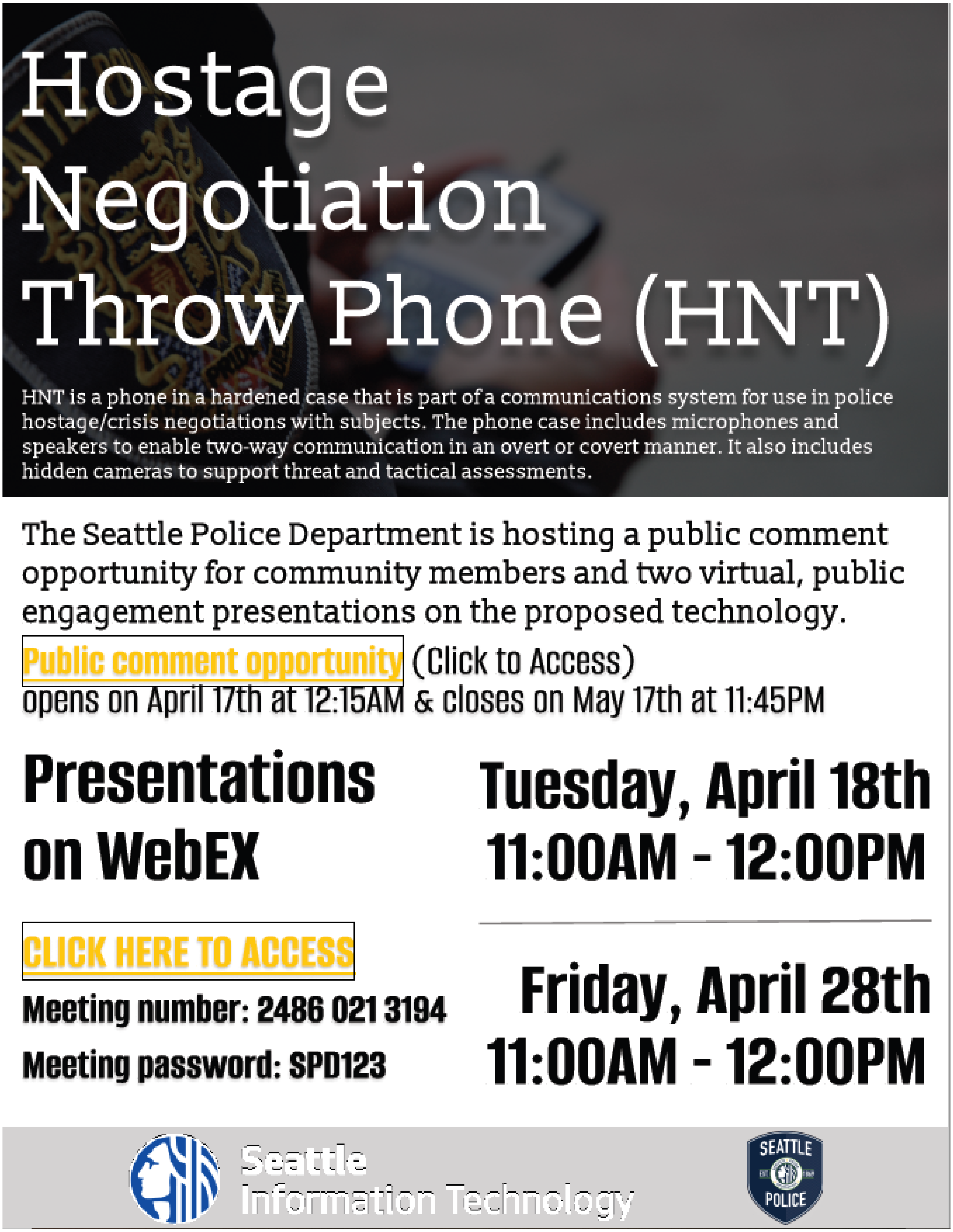
SIR: "surveillance impact report", a document which captures the fulfillment of the Council-defined surveillance technology review process, as required by ordinance 125376.

Workforce equity: (taken from the racial equity toolkit.) Ensure the City's workforce diversity reflects the diversity of Seattle.

Appendix B: Questions and Department Responses

Questions posed by public participants in the first public engagement meeting were answered during the second public comment meeting. These questions and SPD's responses can be found in the Hostage Negotiation Throw Phone Meeting two recording.

Appendix C: Meeting Notice(s)



Hostage Negotiation Throw Phone (HNT)

HNT 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.

The Seattle Police Department is hosting a public comment opportunity for community members and two virtual, public engagement presentations on the proposed technology.

Public comment opportunity (Click to Access)
opens on April 17th at 12:15AM & closes on May 17th at 11:45PM

Presentations on WebEX

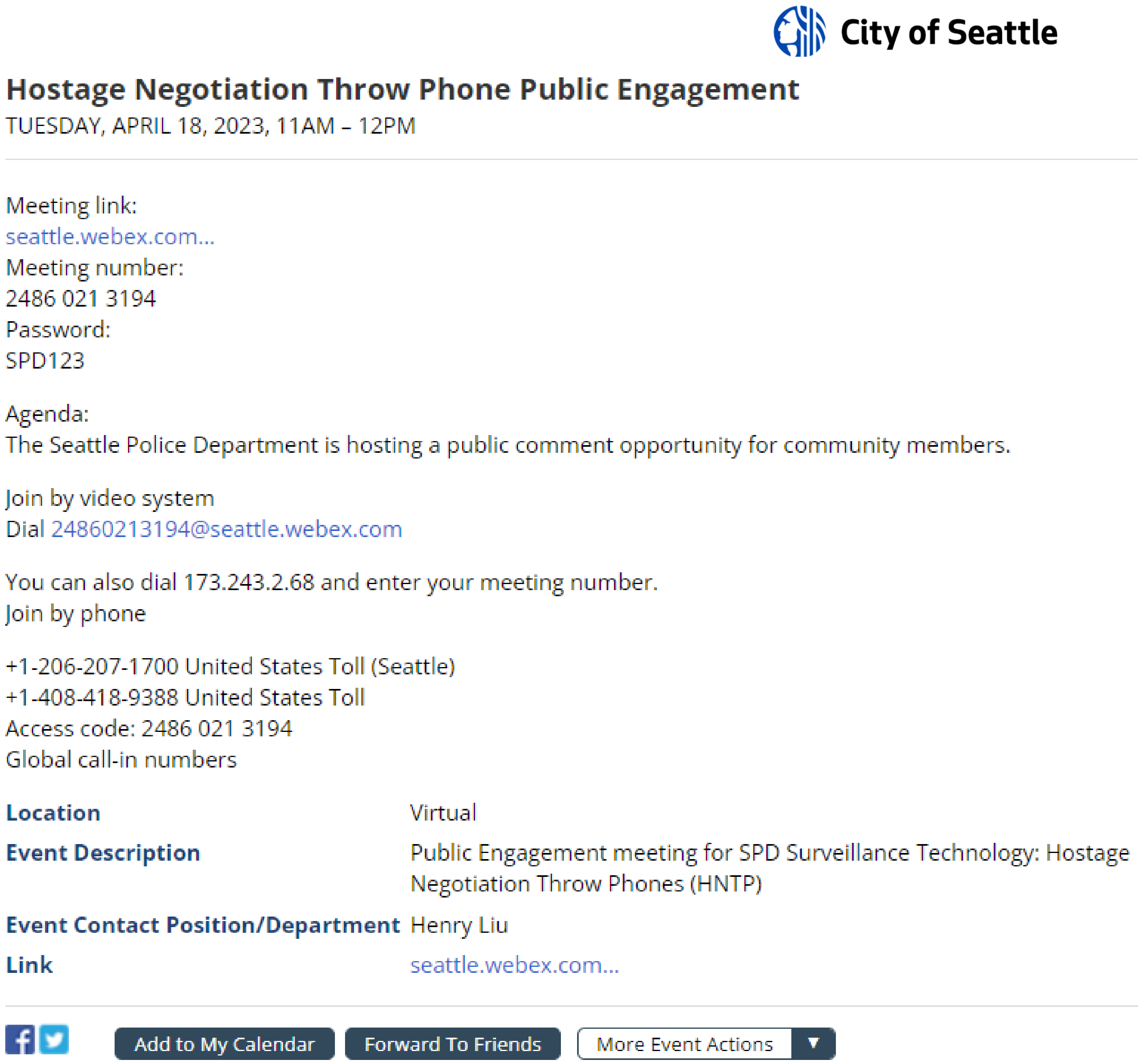
CLICK HERE TO ACCESS

Meeting number: 2486 021 3194

Meeting password: SPD123

Tuesday, April 18th
11:00AM - 12:00PM

Friday, April 28th
11:00AM - 12:00PM



Hostage Negotiation Throw Phone Public Engagement

TUESDAY, APRIL 18, 2023, 11AM – 12PM

Meeting link:
seattle.webex.com...
Meeting number:
2486 021 3194
Password:
SPD123

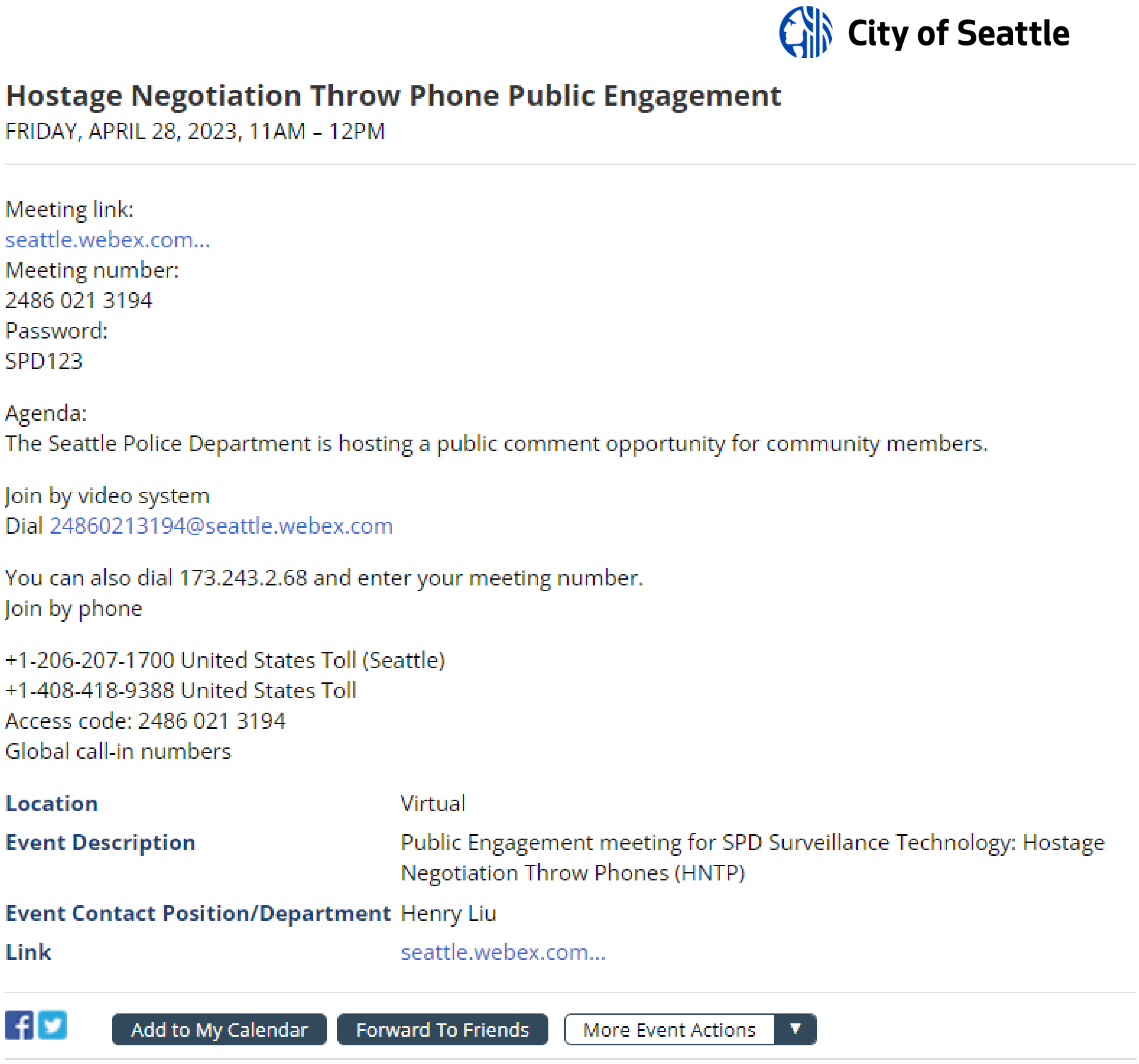
Agenda:
The Seattle Police Department is hosting a public comment opportunity for community members.

Join by video system
Dial 24860213194@seattle.webex.com

You can also dial 173.243.2.68 and enter your meeting number.
Join by phone

+1-206-207-1700 United States Toll (Seattle)
+1-408-418-9388 United States Toll
Access code: 2486 021 3194
Global call-in numbers

Location	Virtual
Event Description	Public Engagement meeting for SPD Surveillance Technology: Hostage Negotiation Throw Phones (HNTP)
Event Contact Position/Department	Henry Liu
Link	seattle.webex.com...



Hostage Negotiation Throw Phone Public Engagement

FRIDAY, APRIL 28, 2023, 11AM – 12PM

Meeting link:
seattle.webex.com...
Meeting number:
2486 021 3194
Password:
SPD123

Agenda:
The Seattle Police Department is hosting a public comment opportunity for community members.

Join by video system
Dial 24860213194@seattle.webex.com

You can also dial 173.243.2.68 and enter your meeting number.
Join by phone

+1-206-207-1700 United States Toll (Seattle)
+1-408-418-9388 United States Toll
Access code: 2486 021 3194
Global call-in numbers

Location	Virtual
Event Description	Public Engagement meeting for SPD Surveillance Technology: Hostage Negotiation Throw Phones (HNTP)
Event Contact Position/Department	Henry Liu
Link	seattle.webex.com...

Appendix D: All Comments Received from Members of the Public

All public comments received can be found in the Public Comment Section 3.0