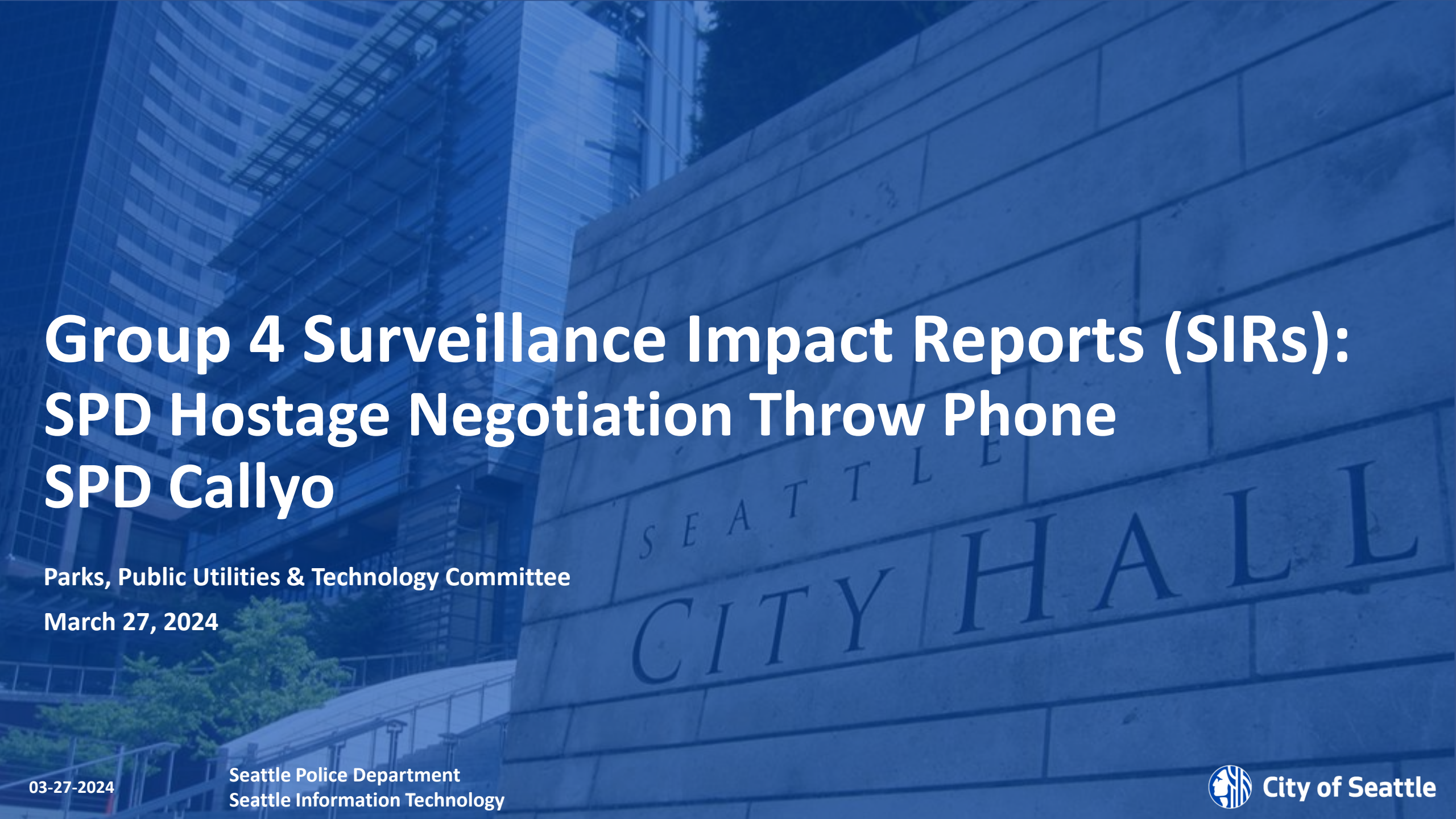

Group 4 Surveillance Impact Reports (SIRs): SPD Hostage Negotiation Throw Phone SPD Callyo

Parks, Public Utilities & Technology Committee

March 27, 2024

Seattle Police Department
Seattle Information Technology

City of Seattle

Surveillance Impact Report (SIR) Process Recap

Sarah Carrier, Privacy Program Manager
Eleonor Bounds, Data Privacy & Accountability Strategist

03-27-2024

Seattle Police Department
Seattle Information Technology

City of Seattle

Surveillance Impact Report (SIR) Process

- Submitted for all retroactive and newly proposed technologies that meet the definition and have no exclusion criteria
- Created by the Departments with project management from IT

1. Privacy Impact Assessment
2. Financial Information
3. Racial Equity Toolkit
4. Public Engagement Comments and Analysis
5. Privacy and Civil Liberties Impact Assessment
6. CTO Response
7. Appendices & Supporting Documentation

Surveillance Impact Report (SIR) Process

1) Draft & Review SIRs	2) Public Comment Period	3) Public Comment Analysis	4) Working Group Review	5) CTO Response	6) Executive Overview	7) Council Review
Staff from the department requesting the technology completes SIR content using the SIR template document.	The initial draft released for public review and comment. One or more public meetings will take place to solicit feedback.	City staff compiles public comments and finalizes the SIR content.	The Community Surveillance Working Group reviews each SIR and completes a privacy and civil liberties impact assessment for each SIR.	The CTO responds to the privacy and civil liberties impact assessment.	City staff creates additional Executive Overview version of the SIR for submission to Council (formerly called the Condensed SIR – CSIR)	City Council will decide on the use of the surveillance technology, by full Council vote.

Group 4 SIR Public Engagement

- Group 4 Surveillance Technologies Public Meetings on __
- One Page Flyers
- Online Public Comment Meeting
  - Recorded and posted online

Engagement Method	(Approximate) Number of Individuals Participating	Number of Comments Received	Number of Questions Received
Public Meeting		-	
Online Comments			
Letters	-		
Total			

In process of adding

Seattle Police Department Group 4 SIRs:

SPD Hostage Negotiation Throw Phone
SPD Callyo

Capt. James Britt, SPD

Seattle Police Department Mission

- Prevent crime;
- Enforce the law; and
- Support quality public safety by delivering respectful, professional and dependable police services.

Hostage Negotiation Throw Phone

What is the technology?

- The Hostage Negotiation Throw Phone is part of a communication system used to negotiate with subjects in hostage or crisis situations.
- 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.

Hostage Negotiation Throw Phone

Why does SPD use the technology?

- Throw phone systems of this nature are standard equipment for Hostage/Crisis Negotiation Teams throughout the country.
- At times there are no other means of phone communication with the subject in a hostage or barricaded person situation.
- The system allows the team to facilitate the development of negotiation strategies and ensure the safety-related information is relayed.

Hostage Negotiation Throw Phone

Data Collection

- Delivery of the throw phone is typically pre-negotiated with the subject via hailing or other means.
- 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 Wi-Fi system.
- Video recorded on the system hard drive is only accessible by HNT members who have controlled access either by password or by permission granted from the computer running the software.

Hostage Negotiation Throw Phone

Protections

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

Hostage Negotiation Throw Phone

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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

Callyo

What is the technology?

- Callyo is a cell phone identification masking and recording technology.
- Callyo is installed on a cell phone and can disguise the identity of an officer by masking a phone number, record phone conversations, and GPS locate identifiable individuals, who are unaware of the operation.

Callyo

Why does SPD use the technology?

- Callyo allows SPD to mask the phone number of a willing participant in an undercover investigation and records conversations and locations of suspects.
- The High Risk Victims Unit uses Callyo to mask phone numbers but does not utilize the recording features of Callyo.
- Audio recording by Callyo and phone number masking contribute to crime reduction by assisting in collecting evidence related to serious and/or violent criminal activity as part of the investigation of criminal activity.

Callyo

Data Collection

- When Callyo is utilized to record, it collects conversations and sounds of individuals related to a criminal investigation.
- Data collected by Callyo is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.
- After having established probable cause, officers make a verbal request to the Technical Electronic Support Unit (TESU) for deployment of Callyo. TESU documents the equipment requested, the legal authority, and the case number.

Callyo

Protections

- Audio recording devices are utilized only after legal standards of consent and/or court-issued warrant have been met, as required by the Washington Privacy Act, Chapt. 9.73 RCW.
- Deployment of audio recording devices is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection.
- All deployments of audio recording devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.

Callyo

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- SPD Policy 5.001 – Standards and Duties
- SPD Policy 5.002 – Responsibilities of Employees Concerning Alleged Policy Violations
- SPD Policy 5.140 – Bias-Free Policing
- SPD Policy 6.060 – Collection of Information for Law Enforcement Purposes
- SPD Policy 7.010 – Submitting Evidence
- 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 Policy 12.111 – Use of Cloud Storage Services

Questions