Group 4B Surveillance Impact Reports (SIRs):

SPD Camera Systems - Images or Non-Auditory Video Recordings
SPD Computer, Cellphone, & Mobile Device Extraction Tools
SPD Crash Data Retrieval Tools
SPD GeoTime
SPD Remotely Operated Vehicles (ROVs)
SPD Tracking Devices

Economic Development, Technology & City Light Committee

February 8, 2023

Seattle Police Department
Seattle Information Technology

City of Seattle

Quick Recap of SIR Process

Ginger Armbruster, Chief Privacy Officer
Sarah Carrier, Privacy Program Manager
Eleonor Bounds, Data Privacy & Accountability Strategist

02-08-2023

Seattle Police Department
Seattle Information Technology

City of Seattle

Surveillance Criteria

Definition: *Technology whose primary purpose is to observe or analyze the movements, behavior, or actions of identifiable individuals in a manner that is reasonably likely to raise concerns about civil liberties, freedom of speech or association, racial equity or social justice. Identifiable individuals also include individuals whose identity can be revealed by license plate data when combined with any other record.*

Exclusions

- Consents to provide the data
- Opt-out notice
- Body-worn cameras
- Police vehicle cameras
- Cameras installed pursuant to state law…or to record traffic violations
- Security cameras
- City infrastructure protection cameras
- Technology that monitors only City employees

Inclusions

- Disparately impacts disadvantaged groups
- PII shared with non-City entities that will use the data for a purpose other than providing the City with a contractually agreed-upon service
- Collects data that is personally identifiable even if obscured, de-identified, or anonymized after collection
- Raises reasonable concerns about impacts to civil liberty, freedom of speech or association, racial equity, or social justice

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

General SIR Creation Timeline

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	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 Surveillance Advisory Working Group reviews each SIR, complete an Assessment included in SIR submission	The CTO responds to the Privacy and Civil Liberties Assessment.	City Staff creates condensed 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.

8-9 months

SIRs Completed from original Master List

Group	Depts.	18 Technologies Completed		Council Bill	Status
Group 1	SDOT	• License Plate Readers • Closed Circuit Television Equipment "Traffic Cameras"	☑	CB 119519 CB 119519	Completed
Group 2	SCL SFD SPD	• Binoculars/Spotting Scope • Check Meter Device • SensorLink Amp Fork • Computer-Aided Dispatch • 911 Logging Recorder • Automated License Plate Reader • Parking Enforcement Systems including Automated License Plate Reader • Computer-Aided Dispatch • CopLogic	☑	CB 120002 CB 120002 CB 120002 CB 120003 CB 120024 CB 120025 CB 120026 CB 120027 CB 120028	Completed
Group 3	SPD	• Forward Looking Infrared Real-time video (FLIR) • Situational Awareness Cameras Without Recording • Video Recording Systems	☑	CB 120053 CB 120054 CB 120055	Completed
Group 4A	SFD SDOT SPD SPD SPD	• Emergency Scene Cameras, Hazmat Camera • *Acyclica • Audio Recording Systems • *Maltego • IBM i2 iBase	☑	CB 120171 Memo CB 120307 CB 120308 CB 120309	Completed 9/15/21, 1/4/22 Completed Completed

Remaining SIRs from original Master List

Group	Depts.	8 Technologies Remaining	Council Bill	Status
Group 4B	SPD	• Camera Systems - Images or Non-Auditory Video Recordings • Computer, cellphone and mobile device extraction tools • Crash Data Retrieval Tools • GeoTime • Remotely Operated Vehicles (ROVs) • Tracking Devices	CB 120499 CB 120501 CB 120500 CB 120502 CB 120503 CB 120504	In Committee
Group 4A Group 4B	SPD SPD	• Callyo • Hostage Negotiation Throw Phone		SPD will transmit in Q2

Group 4B SIR Public Engagement

- Group 4b Surveillance Technologies Public Meetings on April 27, 2022 and May 18, 2022
- 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	12	-	25
Online Comments	-	10	58
Letters	-	2	102
Total	12	12	185

Seattle Police Department Group 4B SIRs

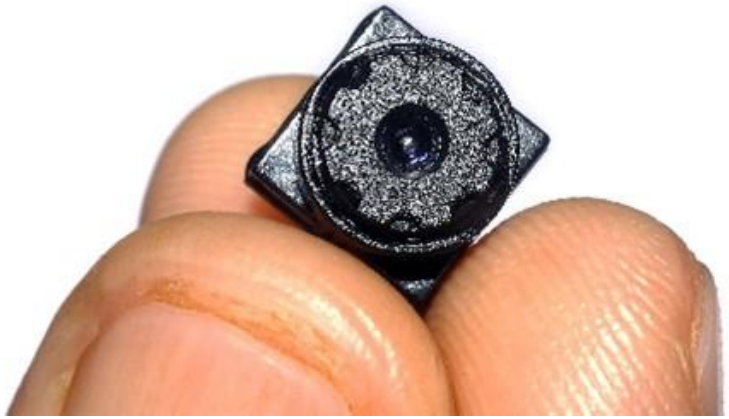
SPD Camera Systems - Images or Non-Auditory Video Recordings
SPD Computer, Cellphone, & Mobile Device Extraction Tools
SPD Crash Data Retrieval Tools
SPD GeoTime
SPD Remotely Operated Vehicles (ROVs)
SPD Tracking Devices

Capt. James Britt, SPD

Camera Systems - Images or Non-Auditory Video Recordings

What is the technology?

- SPD's covert camera systems capture images and video of identifiable individuals, some of whom are unaware of the recording.
- Covert cameras can be concealed on a person or hidden in or on objects within a particular environment. These cameras capture images only, they do not record sound.



Why do we use the technology?

- Covert camera systems are used by the Seattle Police Department (SPD) to obtain information during criminal investigations. These cameras are disguised and used to record specific events related to an investigation.

Camera Systems - Images or Non-Auditory Video Recordings

Data Collection

- When reasonable suspicion of criminal activity exists, cameras may be placed to capture plain view events in areas where no reasonable expectation of privacy exists.
- When placed in areas where a reasonable expectation of privacy exists, use of the camera systems is pursuant to the Washington Privacy Act, Chapt.9.73 RCW, and are utilized only after obtaining appropriate consent and/or legal search warrant authority.

Protections

- All deployments of these devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.
- All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy."

Camera Systems - Images or Non-Auditory Video Recordings

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- Washington Public Records Act, Chapter 42.56 RCW
- WAC 446-20-260
- RCW 10.97.030
- 8 CFR Part 20
- 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

Computer, Cellphone, & Mobile Device Extraction Tools

What is the technology?

- Computer, cellphone, and mobile device extraction tools are used to pull private information from the devices of individuals.
- The different extraction tools SPD utilizes for mobile devices work similarly to one another – a mobile device is physically connected to a computer workstation with specialized locally installed software or to a stand-alone device with a similar software installed.
- The software is able to bypass/decipher/disable the device's PIN/password and extract files containing data from the mobile device.

Why do we use the technology?

- SPD utilizes electronic device extraction and imaging technologies to recover digital information or data from computers, cell phones, and mobile devices as part of a criminal investigation. These technologies are utilized only with the device owner's consent or pursuant to search warrant authority.
- Extraction tools allow investigators to legally collect evidentiary information for ongoing investigations that may be used to prosecute crimes. These tools allow investigators to extract data quickly and securely from a wide variety of devices and preserve evidence from these devices in forensically sound conditions which can then be presented in court.

Computer, Cellphone, & Mobile Device Extraction Tools

Data Collection

- Data extraction devices are utilized only after legal standards of consent or court-issued warrant have been met. Extraction tools for mobile devices, excluding computer imaging, collect information from electronic devices, including contact lists, call logs, Short Messaging Service (SMS) and Multi-Media Messaging Service (MMS) messages, and GPS locations.
- Computer imaging collects an entire image of a computer's hard drive at a specific point in time. Data collected from the extractions is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.

Protections

- All device utilization is documented and subject to audit by the Office of Inspector General and the federal monitor at any time.
- All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon "individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual's right to privacy."

Computer, Cellphone, & Mobile Device Extraction Tools

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- Washington Public Records Act, Chapter 42.56 RCW
- WAC 446-20-260
- RCW 10.97.030
- RCW 9.73.210
- 8 CFR Part 20
- 5.001 - Standards and Duties
- 5.002 - Responsibilities of Employees Concerning Alleged Policy Violations
- 5.140 - Bias-Free Policing
- 6.060 - Collection of Information for Law Enforcement Purposes
- SPD Manual Title 7 – Evidence and Property
- SPD Policy 12.040 - Department-Owned Computers, Devices & Software
- SPD Policy 12.050 - Criminal Justice Information Systems
- SPD Policy 12.055 - Criminal Justice Research
- 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

Crash Data Retrieval Tools

What is the technology?

- Crash Data Retrieval (CDR) tools are important technology used to aid investigators in the reconstruction of traffic collisions. Nearly all passenger vehicles sold in the US since 2013 has an onboard Event Data Recorder (EDR) which automatically records important technical information during a critical event such as a collision.
- These EDR units only record information when certain events occur, such as when airbags deploy or when sensors detect a collision and do not have interfaces which display the information. These tools allow investigators to download and view this information.

Why do we use the technology?

- SPD utilizes CDR tools in the reconstruction of traffic collisions. These tools allow investigators access to information recorded by vehicles around the time of critical events that are associated with vehicle collisions.
- The CDR technology utilized by SPD is required to download and view any data recorded by the EDR units.

Crash Data Retrieval Tools

Data Collection

- CDR tools collect information stored in vehicle EDR units. These tools are utilized only after legal standards of consent and/or court-issued warrant have been met in the investigation of a traffic collision.
- SPD uses CDR tools when it investigates collisions involving specific circumstances such as the death of any person, life-threatening injuries, hit and run collisions, collisions involving substantial bodily injury where it appears a driver was negligent or under the influence of alcohol and or other drugs, vehicular homicide, felony eluding, felony DUI, and other vehicular crimes.

Protections

- CDR Tools 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. Use of CDR Tools is constrained to the conditions stipulated by consent and/or court order, which provides the legal authority and the scope of collection.
- All uses of CDR Tools are documented and subject to audit by the Office of Inspector General and the federal monitor at any time.

Crash Data Retrieval Tools

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- Washington Public Records Act, Chapter 42.56 RCW (“PRA”)
- WAC 446-20-260
- RCW 10.97.030
- 8 CFR Part 20
- 5.001 - Standards and Duties
- 5.002 - Responsibilities of Employees Concerning Alleged Policy Violations
- 5.140 - Bias-Free Policing
- 6.060 - Collection of Information for Law Enforcement Purposes
- SPD Manual Title 7 – Evidence and Property
- SPD Policy 12.040 - Department-Owned Computers, Devices & Software
- SPD Policy 12.050 - Criminal Justice Information Systems
- SPD Policy 12.055 - Criminal Justice Research
- 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

GeoTime

What is the technology?

- GeoTime is geospatial analysis software that allows the visual analysis of events over time. Utilizing geodata, such as latitude and longitude, procured during criminal investigations, investigators use GeoTime to create specialized 2 and 3 dimensional maps of call records and cell site locations.
- These maps allow investigators to see patterns in the existing data that might not be interpreted through other methods.

Why do we use the technology?

- Visualizing criminal information provides investigators a more thorough understanding of complicated criminal investigations.
- GeoTime reduces the time and effort required of investigators to analyze large amounts of data which translates into a better and more efficient work product.

GeoTime

Data Collection

- GeoTime does not collect information or data. It is a tool used to aggregate and analyze data manually input by investigators and exports complex geospatial maps which users save into locally stored investigation files. No information is saved inside the GeoTime tool.

Protections

- GeoTime is only used during the investigation of crimes by the SPD.
- All use of GeoTime must also comply with SPD Policy 12.050 – Criminal Justice Information Systems and may only be used for legitimate criminal investigative purposes.
- Use of GeoTime is governed by the City of Seattle Intelligence Ordinance, 28 CFR Part 23, CJIS requirements, and any future applicable requirements.

GeoTime

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- Washington Public Records Act, Chapter 42.56 RCW ("PRA")
- WAC 446-20-260
- RCW 10.97.030
- 8 CFR Part 20
- 5.001 - Standards and Duties
- 5.002 - Responsibilities of Employees Concerning Alleged Policy Violations
- 5.140 - Bias-Free Policing
- 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 12.055 - Criminal Justice Research
- 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

Remotely Operated Vehicles (ROVs)

What is the technology?

- Remotely Operated Vehicles (ROVs) are unarmed remote controlled vehicles utilized by SPD SWAT, Arson/Bomb, and Harbor units to access areas that are potentially dangerous for personnel to physically enter.
- All SPD ROVs are controlled by SPD employees operating handheld controllers from a safe position nearby. Some ROVs operated by SPD have a remotely controlled arm capable of performing simple tasks safely from a remote location.

Why do we use the technology?

- The use of ROVs allows tactical units to assess potentially dangerous situations from a safe position. By entering an environment with the additional information obtained using remote cameras, or having rendered-safe a suspicious package, SPD personnel and community members are safer.
- The Harbor unit utilizes the ROVs to perform necessary underwater search and recovery functions that would not be possible with manned diving alone.

Remotely Operated Vehicles (ROVs)

Data Collection

- No images or data are stored or retained by ROVs used by the SWAT or Arson/Bomb units. The Harbor unit ROVs store video and sonar imagery captured during each deployment of the unit.
- Only images directly related to the specific search and recovery are manually exported from the ROV's onboard hard drive if requested by SPD detectives for follow up investigation.

Protections

- There is no legal standard or condition for the use of these ROVs in non-protected public areas, such as a hotel hallway or public waterway.
- However, if the use of the ROV is to occur inside a protected area, such as in a person's home or property, absent exigent circumstances, or consent, a signed warrant is obtained from a judge.

Remotely Operated Vehicles (ROVs)

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- Washington Public Records Act, Chapter 42.56 RCW
- WAC 446-20-260
- RCW 10.97.030
- 8 CFR Part 20
- 5.001 - Standards and Duties
- 5.002 - Responsibilities of Employees Concerning Alleged Policy Violations
- 5.140 - Bias-Free Policing
- 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 12.055 - Criminal Justice Research
- 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

Tracking Devices

What is the technology?

- Geolocation trackers are cellular devices that SPD utilizes as a tool to locate and track the movements and locations of vehicles.
- These trackers are location tracking devices that report latitude and longitude as well as other device information such as high temperature alerts, device removal, power/shut down alerts, and battery level.

Why do we use the technology?

- The primary benefit of these tracking systems is in the gathering of evidence used in the resolution of criminal investigations. Proper gathering of location evidence of criminal activity by the police supports SPD's mission to prevent crime, enforce the law, and support quality public safety.
- Trackers allow SPD to remotely track vehicles electronically. They also allow SPD to locate vehicles and individuals that are sought in connection with an active investigation. They are only utilized with consent of a witness, a confidential informant, or within the scope of a judicially issued search warrant.

Tracking Devices

Data Collection

- Tracking devices are only utilized with express consent or search warrant authority. These devices report latitude and longitude coordinates on a pre-determined schedule that can be adjusted by users remotely.
- Data collected from the tracking devices is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.

Protections

- All deployments of these devices are documented by TESU and subject to audit by the Office of Inspector General and the federal monitor at any time.
- All information must be gathered and recorded in a manner that is consistent with SPD Policy 6.060, such that it does not reasonably infringe upon “individual rights, liberties, and freedoms secured by the Constitution of the United States and of the State of Washington, including, among others, the freedom of speech, press, association and assembly; liberty of conscience; the exercise of religion; and the right to petition government for redress of grievances; or violate an individual’s right to privacy.”

Tracking Devices

Related Policies

- Washington Privacy Act, Chapt.9.73 RCW
- Washington Public Records Act, Chapter 42.56 RCW ("PRA")
- GS2016-009 - Washington State Retention Schedule for Records Documented
- SMC 14.12
- 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 12.055 - Criminal Justice Research
- 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