

# Surveillance Technology Public Comment Meeting

Seattle Police Department



# Public Records Act Notice

- This meeting is being recorded and will be posted online
- Information provided (including public comments) to the City of Seattle is considered a public record and may be subject to public disclosure. For more information see the [Public Records Act, RCW Chapter 42.56.](#)

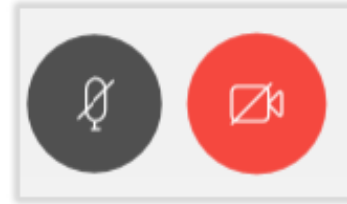


# WebEx Basics

## Participant Etiquette

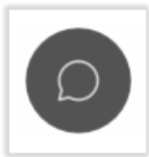
Manage your audio and video appropriately. It is good Webex etiquette to mute your line when you are not speaking. The microphone icon will be **RED** when muted.

Using video in a meeting can help teams stay connected and aligned as well as improve overall communication. Sometimes though, video can be distracting. To mute your video, click the video icon. The icon will be **RED** when muted.

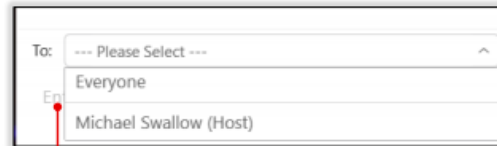


## Chatting

Select the Chat icon on the tool bar at the bottom of the screen.

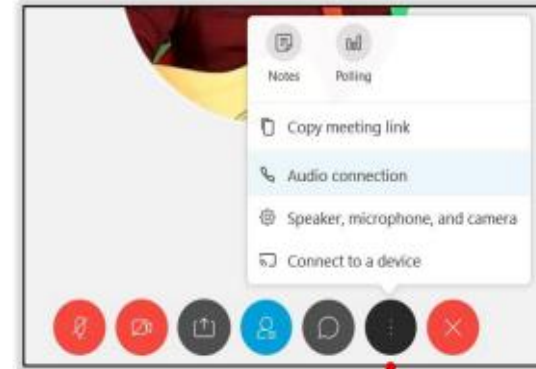


Select the drop box.

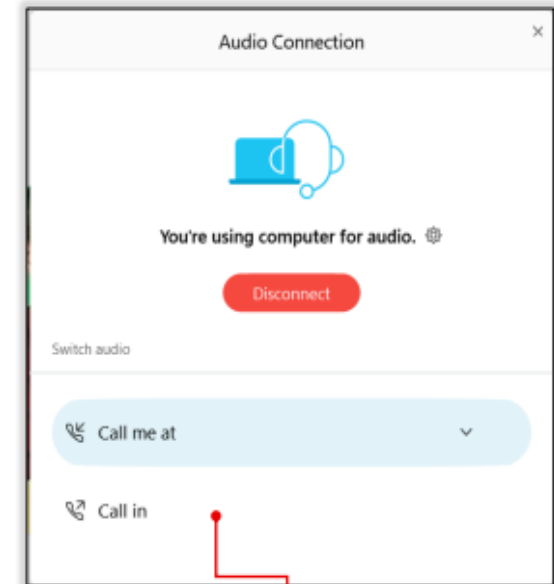


Select if you would like to send your message to **Everyone** or to a specific individual. If you select a specific individual, this will send the message privately so no one else in the meeting will see it.

## Troubleshooting Audio



If you are having audio issues, click on the **ellipsis (...)**. You can test your **speakers, microphone, and camera** here, or select **Audio Connection** to change the way you are connected.



Select from the available options to change your audio connection.

# WebEx Basics

## For Dial-In Attendees

- Once the meeting starts, if you have a question, press “\*3” to raise your hand. Once you have raised your hand, you'll hear the prompt, "You have raised your hand to ask a question. Please wait to speak until the host calls on you."
- To hear a list of commands available during your meeting or event, press “\*\*”.
- If you no longer want to ask a question, or the host has already called on you, then press “\*3” to lower your hand. You will hear a message, "You have lowered your hand".



# Ground Rules

**Attendees will be asked to adhere to the surveillance public meeting code of conduct:**

- ✓ Be respectful of diverse opinions and experiences.
- ✓ Be an active listener during presentations.
- ✓ Anyone exhibiting disruptive behavior, intimidation or aggression, may be muted. If so, they will be asked to provide comment online or by letter.
- ✓ Please keep comments as brief as possible and related to technologies in focus to allow everyone an opportunity to speak.

# City of Seattle's Definition of Surveillance

- Surveillance is defined as technologies that "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."
- Certain technologies, such as police body cameras and technologies for everyday office use, are excluded from the law.

# How to Comment on Technologies

- Survey Link: <https://seattle.surveymonkey.com/r/BPF6GKM>
- Mail a comment to Surveillance & Privacy Program:  
Seattle IT  
PO Box 94709  
Seattle, WA 98124



# Rundown of Events

- SPD will present on technologies currently in use
  - 1) Camera systems
  - 2) Tracking Devices
  - 3) Remotely Operated Vehicles (ROVs)
  - 4) GeoTime
  - 5) Computer, cellphone and mobile device extraction tools
  - 6) Crash Data Retrieval
- Public Dialog Opportunity





# Additional Comments

For additional comments unrelated to these specific surveillance technologies, please utilize the following resources:

- [Find Your Council District / Councilmember](#)
  - Contact City Council at [council@seattle.gov](mailto:council@seattle.gov)
- [SPD Contact Information](#)



The image shows a low-angle shot of the Seattle City Hall building, characterized by its curved facade and stone masonry. The building's name, "SEATTLE CITY HALL", is visible in large, raised letters on the stone surface. The entire image is overlaid with a semi-transparent blue filter. Centered on the image is the text "Group 4b Technologies" in a bold, white, sans-serif font, with "Seattle Police Department" in a slightly smaller, white, sans-serif font directly below it.

**Group 4b Technologies**  
Seattle Police Department

# Seattle Police Department Mission

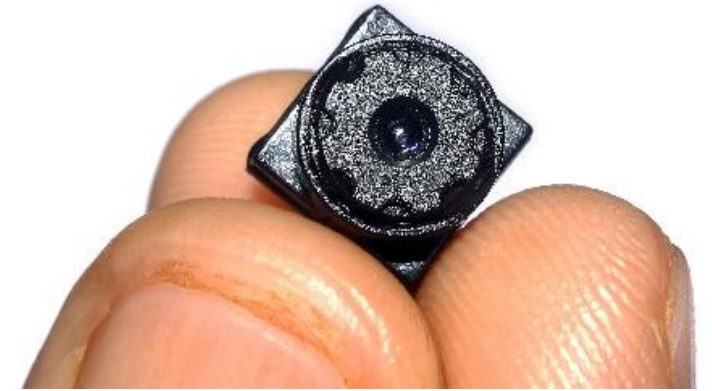
- **Prevent crime;**
- **Enforce the law; and**
- **Support quality public safety by delivering respectful, professional and dependable police services.**



# Camera Systems

## 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.



# Camera Systems

## Why does SPD 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

## 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.

# Camera Systems

## 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

## 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

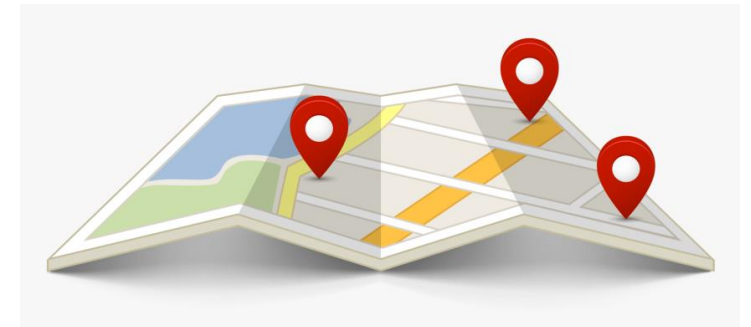




# Tracking Devices

## 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.



# Tracking Devices

## Why does SPD 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.

# Tracking Devices

## 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



# 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.



# Remotely Operated Vehicles (ROVs)

## Why does SPD 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.



# Remotely Operated Vehicles (ROVs)

## 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



# 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.



# GeoTime

## Why does SPD 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.

# GeoTime

## 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



# Computer, cellphone and 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.





# Computer, cellphone and mobile device extraction tools

## Why does SPD 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 and 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.

# Computer, cellphone and mobile device extraction tools

## 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 and 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

## 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.



# Crash Data Retrieval

## Why does SPD 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

## 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.

# Crash Data Retrieval

## 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

## 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



# Public Comment



Please use the “raise hand” feature and we will call on individuals one at a time for questions



The Q&A feature will also be open for questions or comments at this time

# What's Next?

- Visit the [Group 4b Technologies Survey](#) to submit comments about these technologies
- Comments collected will be included in the SIR submitted to the Surveillance Advisory Working Group, and then City Council for full Council vote.
- [Seattle.gov/tech](http://Seattle.gov/tech) - leave a comment on the Tech Talk Blog

**Thank you for attending.**

SEATTLE  
CITY HALL