Surveillance Technology Public Comment Meeting

Seattle Police Department

Public Records Act Notice

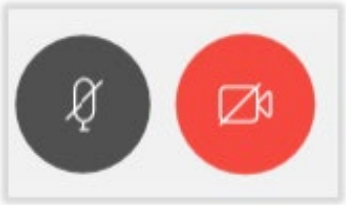
- This meeting is being recorded and will be posted online

- 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.

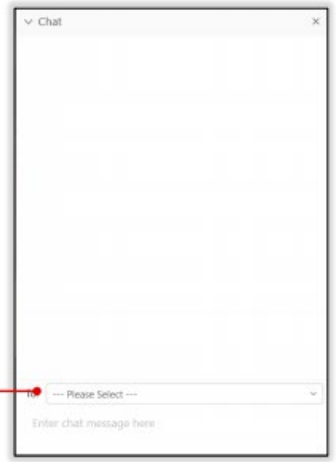


Using video in a meeting can help teams stay connected and aligned as well as improve overall communication. Sometimes though, video can be distracting. To mute your video, click the video icon. The icon will be RED when muted.

Chatting

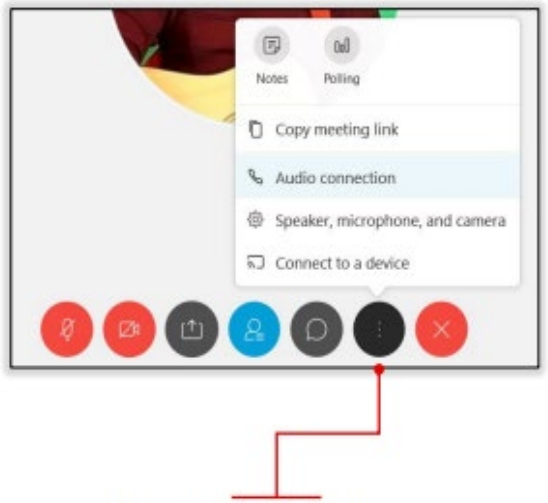
Select the Chat icon on the tool bar at the bottom of the screen.

Select the drop box.

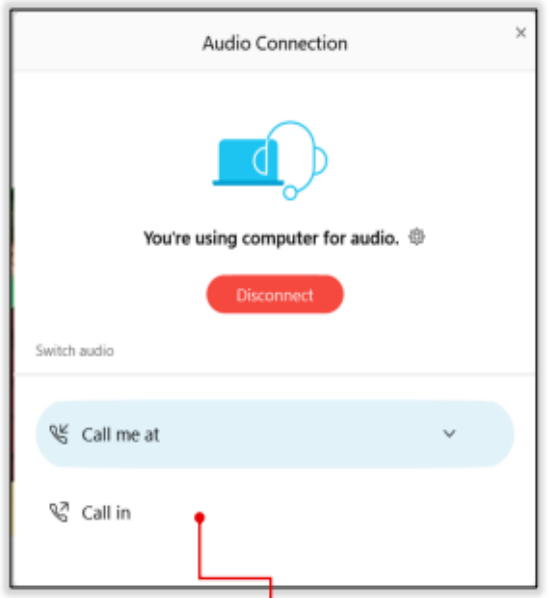


Select if you would like to send your message to **Everyone** or to a specific individual. If you select a specific individual, this will send the message privately so no one else in the meeting will see it.

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.

City of Seattle

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/HR2FDDD
- 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
  - Audio Recording
  - Callyo
  - I2 iBase
  - Maltego
- Public Comment 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
- SPD Contact Information

Group 4a 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.

Audio Recording Systems

What is the technology?

- Audio recording devices are typically known as “wires” and can be concealed on a person or hidden in or on objects within a particular environment.
- Audio recording devices must be turned on by an individual and they record only portions of a conversation that occur while the device is on.

Audio Recording Systems

Why does SPD use the technology?

- Audio recording systems 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.
- Audio recording systems allow SPD to pursue resolution of criminal investigations expeditiously by recording conversations of suspects, once an appropriate determination that sufficient probable cause exists has been made and a warrant has been issued.

Audio Recording Systems

Data Collection

- All audio recording systems utilized by SPD are managed and maintained with the Technical and Electronic Support Unit (TESU).
- Data collected from audio recording devices is provided to the requesting Officer/Detective for inclusion in the investigation file and is stored following evidence guidelines.

Audio Recording Systems

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.

Audio Recording Systems

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

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 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

Link Analysis - IBM I2 iBase

What is the technology?

- I2 iBase is a link analysis software used to combine data stored in SPD criminal information systems with information gathered during criminal investigations and display that information on a link chart.

- A virtual “pin board,” helping investigators to visualize the connections between known entities, vehicles, locations, etc. in the course of a criminal investigation.

Link Analysis - IBM I2 iBase

Why does SPD use the technology?

- IBM i2 iBase is used by analysts within the Real Time Crime Center (RTCC) to assist with criminal investigations and to provide actionable information to units in the field.
- Visualizing criminal information provides investigators a more thorough understanding of complicated criminal investigations.

Link Analysis - IBM I2 iBase

Data Collection

- The iBase application imports specific data elements related to the investigation from SPD's Records Management System (RMS) and Computer Aided Dispatch (CAD) system.
- Users may also manually add additional information that they have collected during the course of a criminal investigation to assist in understanding complex investigations.

Link Analysis - IBM I2 iBase

Protections

- Only authorized users can access the system, technology, or the data. Access to the iBase system requires SPD personnel to log in with password-protected login credentials. All of these employees are ACCESS and Criminal Justice Information System (CJIS) certified.
- The I2 iBase system is CJIS compliant. The software also logs user sign on/off, each time a user accesses any piece of data, and any additions or changes a user makes.

Link Analysis - IBM I2 iBase

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
- City of Seattle Intelligence Ordinance, 28 CFR Part 23

Link Analysis - Maltego

What is the technology?

- Maltego is an Open-Source Intelligence (OSINT) platform which presents publicly available information in an easy to interpret visual entity-relationship model which allows investigators to analyze connections between individuals related to criminal investigations.
- Maltego queries public data on the internet, such as domains, and displays it in a diagram showing links.

Link Analysis - Maltego

Why does SPD use the technology?

- Maltego is a popular tool that is used across the information-security community for both defensive cyber-security programs and for investigating breaches and instances of cyber-crime.
- A useful tool used in cyber-crime investigations, as these incidents often involve interactions between individuals, devices, and networks that are otherwise unknown.

Link Analysis - Maltego

Data Collection

- Maltego queries publicly available data on the internet and collects information based on the parameters of the search request entered by a detective, much like Google returns results based on specific search terms.
- SPD utilizes Maltego to investigate cybercrimes, primarily in determining the digital origin of attacks against cyber infrastructure.

Link Analysis - Maltego

Protections

- Access to Maltego is restricted to use for the related security incident and/or pertinent criminal investigations and subject to Department Policy regarding ongoing criminal investigations.
- Maltego is used by two trained TESU detectives within TESU, and by no other entity. Use of Maltego is governed by SPD Policy, the City of Seattle Intelligence Ordinance, 28 CFR Part 23, and CJIS requirements.

Link Analysis - Maltego

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
- City of Seattle Intelligence Ordinance, 28 CFR Part 23

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 4a 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 - leave a comment on the Tech Talk Blog

Thank You

For Attending