



# St. Louis Metropolitan Police Department Surveillance Use Plan



## SURVEILLANCE TECHNOLOGY:

In-Car Cameras

## DESCRIPTION:

*Information describing the surveillance technology and how it works, including product descriptions from manufacturers*

The St. Louis Metropolitan Police Department utilizes In-Car Cameras (ICCS) as a part of the visual and audio recording of police interactions with the public and to provide more transparency around police-citizen interactions. In-car cameras are able to capture images of people, vehicles, locations, license plates, and other visual information. In-car cameras can also capture acoustic data that occurs within range of the device.

The in-car cameras are mounted in the fleet vehicles and are mounted to either the front windshield or the dashboard. In-car cameras capture and record video of what occurs in front of the vehicle. Once the vehicle is started the

Once the vehicle is started the camera is turned on and is in a “buffering” mode, which means that the camera is recording, but it is re-writing over the data in pre-set intervals. Long-term recording automatically begins when the employee operating the vehicle activates the light bar, is moving at speeds over 70 mph, removes the shotgun for the rack, or opens the driver’s side door with the light bar activated. When the employee terminates all of the previously mentioned conditions, the recording is deactivated, and the in-car camera returns to the buffering state. This process is repeated until the vehicle is returned to its area station.

ICCs have become a vital tool in improving and enhancing the safety of officer and civilian interactions, in addition to evidence collection. ICCs assist with incident reviews by supervisors, ensure accountability, encourage lawful and respectful interactions between the public and the police, and assist in de-escalation of possibly volatile encounters.

ICCs cannot be used to edit recorded videos. SLMPD ICCs do not use facial recognition technologies and cannot conduct a facial recognition analysis. However, a still image can be created from an ICCs video image and may be used as a probe image for facial recognition analysis.

The SLMPD strives to maintain the highest standards of honor and integrity. SLMPD is committed to building trust with all members of the community, by respecting and protecting the constitutional rights and dignity of all individuals during law enforcement contacts and/or enforcement actions. *See SLMPD Special Order 1-04 (Prohibition of Bias-Based Policing and Racial Profiling), SLMPD Special Order 1-08 (Interaction with Transgender Individuals), and SLMPD Directive 2021-08-27 (Consent Judgement Respecting Right to Assemble and Engage in Non-Violent Protest and Criticize, Complain About, and Video Record Police).*



# St. Louis Metropolitan Police Department Surveillance Use Plan



## PURPOSE:

### *What specific purpose(s) the surveillance technology is intended to advance*

These devices are used to provide true accounts of officer-civilian interactions. ICCs are also used in documenting scenes, such as crime scenes, accident scenes, or other events like the seizure of property and documenting the custody of such property. These devices allow officers to document interviews, statements, and events during an investigation to assist with the prosecution of cases.

It should be noted that ICCs can only provide a limited view of an incident and other available evidence must be taken into consideration to have a clearer picture of the entire incident, such as witness statements, officer interviews, forensic analysis and other available technology resources. It has also been determined in various studies that the use of ICCs help reduce the number of complaints filed against police officers, increase police accountability, and increase transparency resulting in enhanced public trust.

## AUTHORIZED USE(S):

*For what specific capabilities and uses of the surveillance technology is authorization being sought, including amounts, to be acquired and deployed, expected geographic areas and durations, organizational partnerships, and Memorandums of Understanding (MOUs) and:*

- 1) SLMPD is requesting the continued use of ICCs to record/document officer-civilian interactions.
- 2) SLMPD currently has 200 ICCs. The department has an RFP out seeking to purchase 300 ICCs, which will outfit the patrol fleet.
- 3) Currently the department has 200 in-car cameras, but 300 in-car cameras are being sought to equip all patrol vehicles with this technology.
- 4) SLMPD does not have any organizational MOUs or partnerships for these technologies.

***a) What legal and procedural rules will govern each authorized use, including where an application of Surveillance Technology requires a warrant?***

These technologies are governed by departmental policy Special Order 5-33 titled *Body Worn Camera and In-Car Camera System*. The policy states:

- (1) Citizens do not have a reasonable expectation of privacy when talking with police officers during the scope of a police officer's official duties, even when the contact is in a private residence.
- (2) Employees are not required to give citizen notice that they are being recorded, but employees are strongly encouraged to inform citizens they are being recorded to de-escalate potential conflicts.
- (3) If a citizen requests that an employee stop recording during an event for which policy requires recording, the employee will continue to record and explain that Department policy requires recording of the event.



# St. Louis Metropolitan Police Department Surveillance Use Plan



- (4) If a citizen requests that an employee stop recording in a private residence or on other private property AND the employee has no other legal right to be present (e.g., warrant, exigent circumstances) AND the interaction is not contentious or confrontational, the employee will stop recording.
- (5) Any citizen request to stop recording will be recorded prior to stopping the recording.
- (6) Employees will verbally state the reason for stopping recording before recording is terminated.
- (7) In an interaction becomes contentious or confrontational after recording has stopped, employees will resume recording.
- (8) Employees and supervisors involved in the investigation of a complaint against a member of the Department will inform the complainants and complaint witnesses they are being recorded.

The ICC will automatically activate through any of the following (1) light bar activation; (2) vehicle speed (70 mph); (3) shotgun removed from rack; (4) open driver's door when light bar activated.

If the ICC does not automatically activate, employees will manually activate the equipment in the following circumstances:

- (1) Responding to dispatched calls, starting before the employee arrives on scene
- (2) During traffic or other investigative stops
- (3) Anytime the vehicle light bar is activated
- (4) Making an arrest or seizure
- (5) Questioning victims, suspects, or witnesses
- (6) During vehicle or foot pursuits
- (7) During a use-of-force incident or investigation
- (8) Immediately after being involved in a vehicle crash
- (9) Prior to transporting any citizen (except those participating in a ride along)
- (10) During all searches of people, vehicles, or premises conducted with or without a search warrant
- (11) When entering a private residence or business for law enforcement purposes
- (12) Any time the employee believes the recording would be appropriate and beneficial to Department operations

Recordings will be ceased by an employee once their involvement in the event has concluded. Conclusions of the event occurs when (1) all relevant communications with the public have ended; (2) the gathering of evidence is completed; (3) transportation and/or transfer of custody is completed; and (4) the employee reasonably believes further recording will not capture pertinent activities.

***b) What potential uses of the surveillance technology will be expressly prohibited?***

ICCs will not be used to record non-work-related activity.



# St. Louis Metropolitan Police Department Surveillance Use Plan



Employees will not record in sensitive areas, such as restrooms, locker rooms, dressing rooms, detention facilities, mental health or counseling facilities, and medical facilities, unless recording is necessary for law enforcement purposes (e.g., ongoing criminal investigations, crime in progress).

Employees will not record strip searches, tactical briefings, coaching/training sessions, labor union activities, any privileges communications (e.g., attorney/client; doctor/patient), transport of victims to safehouses, contact with confidential informants, courtroom proceedings, department administrative investigations.

Employees will not record people engaged in First Amendment activities (e.g., marches, protests), unless the Bike Response Team or the Civil Unrest Team has been deployed (not simply staged) and the employee has reasonable suspicion to believe unlawful activity is occurring or imminent risk to public safety or property destruction appears likely. During First Amendment activities, employees will have their equipment on and in the “buffering” mode.

Employees will notify the BWC Unit if they record an undercover officer, a confidential informant, or any of the above events. The BWC Unit will flag such videos for proper redaction.

***c) How and under what circumstances will surveillance data that was collected, captured, recorded, or intercepted by the surveillance technology be analyzed and reviewed?***

The use of these technologies is governed by SO 5-33, and circumstances on how and when data can be reviewed are mentioned in Section N (Reviewing BWC/ICC Recordings).

The data recorded by this technology is “accessed only for legitimate law enforcement purposes,” out of public view. Recordings should be reviewed prior to testifying in court for a case, and in cases not being investigated by the Force Investigations Unit, data may be reviewed in preparation of any incident report. Investigators may review ICC, for official criminal or administrative investigations.

Supervisors will review ICC recordings that are use of force incidents not being investigated by the Force Investigations Unit; incidents related to vehicle pursuits; incidents related to an employee’s on-duty injury; or to determine discipline.

Officers are prohibited from viewing BWC/ICC recordings for incidents being investigated by FIU, until a Voluntary Statement is made to FIU. When an officer does review the BWC/ICC for an FIU investigation, it will be done in the presence of the FIU investigator.

## DEPLOYMENT:



# St. Louis Metropolitan Police Department Surveillance Use Plan



*If the surveillance technology will not be uniformly deployed or targeted throughout the city, what factors will be used to determine the specific geographic targeting, and what measures will be taken to ensure such targeting is racially and economically neutral.*

SLMPD currently has 200 ICCs. The department has an RFP out seeking to purchase 300 ICCs, which will outfit the departments patrol fleet.

## **COST:**

*The fiscal impact of the surveillance technology, including costs of technology acquisition, operation, maintenance, personnel, and data storage, as well as all sources of funding and donations.*

Currently ICCs cost \$752,600. An RFP has been issued to increase the number of ICCs the department currently owns. These costs include all maintenance and data storage for the contract period of 5 years, which the current contract is set to end in July of 2025.

## **DISCRIMINATORY IMPACT AVOIDANCE:**

*What specific, affirmative measures will be implemented to safeguard the public from the potential discriminatory impacts of the technology, including without limitation what measures will be used to avoid biases in surveillance targeting and data collection?*

The measures taken to avoid potential discriminatory impacts of the technology is that the technology is installed in all patrol fleet vehicles, which is why the department has an RFP out to ensure that this happens. The current ICCs equipment is deployed evenly throughout the patrol fleet.

## **DATA COLLECTION:**

a) *What types of surveillance data will be collected, captured, recorded, intercepted, or retained by the surveillance technology?*

The data obtained from these technologies include video and audio.

b) *What surveillance data may be inadvertently collected during the authorized uses of the surveillance technology, and what measures will be taken to minimize the inadvertent collection of data?*

When data is inadvertently collected during the authorized use of this technology, the officer will notify the BWC Unit for the video to be flagged for proper redaction of the inadvertently collected data. Inadvertently collected data would be considered any data recorded that is prohibited, recordings of undercover officers, confidential informants, or the employee using the restroom.

Measures taken to minimize the inadvertent collection of data is having audible alerts to advise the officer that recording has begun. ICCs are automatically activated when the vehicles light bar is activated, when the vehicle speed is 70mph, when the shotgun is removed from the rack, or when the driver's doors is opened while the light bar is activated.

c) *How inadvertently collected surveillance data is be expeditiously identified and deleted?*



# St. Louis Metropolitan Police Department Surveillance Use Plan



It is the responsibility of the officer to make the notification to the Commander of the Body Worn Camera Unit to advise if data has been collected inadvertently. There are daily audits of recordings conducted to ensure the recordings are properly classified (by incident type), that recordings are flagged that have captured sensitive or normally prohibited content, and to ensure the proper functioning and use of ICC equipment and to perform a general quality review of agency operations.

**d) *How the City Entity will ensure that, when it retains surveillance data, such retention will comply with the Missouri Records Retention Schedule?***

SLMPDs retention of ICC data is determined by the officer's classification of the type of incident. The classification of an incident means the type of crime or civilian-officer interaction. Retention of each recording is tied to the assigned classification, which corresponds to the State of Missouri's Police Records Retention Schedule.

## **DATA PROTECTION:**

***What safeguards will be used to protect surveillance data from unauthorized access, including encryption and access control mechanisms, and what protocols will be put in place to authorize access and monitor who has access.***

The data can only be accessed through a controlled system that keeps a log of the user accessing the data. Commissioned personnel all can access data related to ICC, but their access has various permission levels. Officers have permission to review their recorded data for reporting purposes or court purposes, supervisors have access to review data for disciplinary reasons and have access to personnel assigned to them, the BWC Unit can access all data to ensure compliance with policies/procedures and to conduct daily audits. The amount of access and protocols for access to the data is governed by SO 5-33.

## **DATA RETENTION:**

***What rules and procedures will govern the retention and deletion of surveillance data, including how it will be ensured that the schedule for retaining and deleting aligns with the guidelines specified in RSMo 109.200-109.310 and how data collected by the City Entity as a result of the use of surveillance technology shall be stored in a manner such that it cannot be modified, destroyed, accessed or purged contrary to the Missouri Police Clerks Records Retention Schedule.***

SLMPDs retention of ICC data is determined by the officer's classification of the type of incident. The classification of an incident means the type of crime or civilian-officer interaction. Retention of each recording is tied to the assigned classification, which corresponds to the State of Missouri's Police Records Retention Schedule. It is the responsibility of the BWC Unit to code retention levels, such that employees may select from a list of types of events to satisfy the classification requirement. Data is purged from the system based on the classification of the incident.

## **SURVEILLANCE DATA SHARING:**





# St. Louis Metropolitan Police Department Surveillance Use Plan



*If a city entity is seeking authorization to share access to surveillance technology or surveillance data with any other persons, city entities, or governmental entities, it shall detail:*

- a) Which persons, city entities, or other governmental entities will be approved for (i) surveillance technology sharing, and for (ii) surveillance data sharing;**

Recordings will be accessed only for legitimate law enforcement purposes. The review of any ICC recordings will occur out of public view. Employees will review their ICC recordings before testifying in court for a criminal case.

All ICC recordings are considered an investigative record and are the exclusive property of the department. Accessing, copying, forwarding, or releasing any digital evidence other than official law enforcement use and contrary to Special Order 5-33 is strictly prohibited. Public release of digital evidence is prohibited unless approved by the Police Commissioner.

Personal computer equipment and software programs shall not be utilized when making copies of digital evidence. Only the BWC Unit has the authority to export ICC videos upon request. Using secondary recording devices such as video cameras, cell phones or other devices to record or capture digital evidence from a departmentally owned computer is strictly prohibited.

- b) How much sharing is necessary for the stated purpose and use of the surveillance technology;**

No sharing is necessary for the use of this technology. All BWC/ICC recordings are considered a record and are the exclusive property of the Department. Accessing, copying, or releasing recordings for non-law enforcement purposes is prohibited, unless otherwise required by law or in conformance with other provisions of SO 5-33.

- c) How will it ensure any person, city entity, or governmental entity approved for access to the surveillance technology or surveillance data complies with the applicable Surveillance Use Plan and does not further disclose the surveillance data to unauthorized persons and entities.**

Only SLMPD employees are authorized access to review the data from BWCs or ICCs. Any violation of SO 5-33 will lead to disciplinary actions.

## DEMANDS FOR ACCESS TO SURVEILLANCE DATA:

*What legal standard must be met by government entities or third parties seeking or demanding access to surveillance data.*

Members of the public may request copies of ICC-recorded video through a Sunshine Request. The SLMPD will review and evaluate such requests in accordance with the applicable provisions of the law and the department's policies.

All BWC recordings are considered an investigative record and are the exclusive property of the department. Accessing, copying, forwarding, or releasing any digital evidence other than official law enforcement use



# St. Louis Metropolitan Police Department Surveillance Use Plan



and contrary to Special Order 5-33 is strictly prohibited. Public release of digital evidence is prohibited unless approved by the Police Commissioner.

Personal computer equipment and software programs shall not be utilized when making copies of digital evidence. Only the BWC Unit has the authority to export ICC videos upon request. Using secondary recording devices such as video cameras, cell phones or other devices to record or capture digital evidence from a departmentally owned computer is strictly prohibited.

## **TRAINING:**

*What training procedures will be implemented to ensure compliance with this ordinance, the Revised Code of the City of St. Louis, and applicable federal and state laws and regulations.*

All personnel are trained in departmentally issued equipment. The BWC Unit is responsible for the training of BWC and ICC usage for all employees. There is no annual training related to the use of BWC/ICC, unless there are legal updates, at which time the entire department will be provided with the training by the BWC Unit.

## **AUDITING AND OVERSIGHT:**

*What mechanisms will be implemented to ensure the Surveillance Use Plan is followed, including what independent or non-independent persons or entities will be given oversight authority, and what legally enforceable sanctions will be put in place for violations of the Plan?*

ICCs are overseen by the BWC Unit, who conducts daily audits to ensure compliance with departmental policies, per SO 5-33. If it is determined that an employee is not following the policies around BWC activation and usage, an internal investigation can be initiated, which can result in disciplinary actions. Employees reviewing recordings should remain focused on the incident(s) in question and review only those recordings relevant to their investigative scope. If potential misconduct is identified, the employee will immediately notify a supervisor. The supervisor will report the potential misconduct to the employee's Commander through the chain of command. Nothing in Special Order 5-33 prohibits a supervisor from addressing policy violations, which can result in disciplinary actions.

## **COMPLAINTS:**

*What procedures will be put in place by which members of the public can register complaints or concerns, submit questions about the deployment or use of a specific surveillance technology, and how the city entity will ensure each question and complaint is responded to in a timely manner.*

Complaints about surveillance technology can be made to the Civilian Oversight Board using the Joint Citizen Complaint Form which can be located [here](#).

Residents are also able to make comments about surveillance technology by contacting the Citizens Service Bureau (314) 622-4800.