St. Louis Metropolitan Police Department

Surveillance Use Plan

SURVEILLANCE TECHNOLOGY:

Cybercrime Technologies - Forensic Examination Hardware and Software

DESCRIPTION:

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

The St. Louis Metropolitan Police Department utilizes hardware and software to conduct forensic examinations of handheld devices, computers, and other electronic equipment, including:

- Mobile devices (Smartphones, Tablets, etc)
- Storage devices (Thumb Drives, External Hard Drives, SD Cards)
- Computers (Macintosh or Windows)
- Network Intrusion Response/Malware Analysis
- Vehicle System Forensics (Infotainment and Telematics Systems)
- Skimmer Forensics
- Drone Forensics

The technologies are used to gather evidence for criminal investigations and the forensic examination of the above listed devices only in exigent circumstances, after obtaining a court ordered search warrant or consent of the owner or user of the device. Exigent circumstances related to this technology are dependent on solving a criminal investigation that could lead to severe concerns related to the larger community's public safety. Common instances of exigent circumstances would be accessing the recovered phone of a victim of a deadly crime, to assist in identifying a suspect, or using the technology to identify the origin of a bomb/school shooting threats.

PURPOSE:

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

The use of these technologies is to gather evidence for criminal investigations. The investigators of the department do not use these technologies to gain unauthorized access to computers, computer services, computer networks, or any other electronic devices. Failure to comply with the policies and procedures of the department will result in disciplinary actions.

SLMPD aims to maintain the highest standard of integrity and is committed to protecting the civil rights and liberties of our community.

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 these technologies to continue to do forensic examinations of devices related to crimes being investigated, in exigent circumstances, after obtaining a court ordered search warrant or consent of the owner or user of the device.
2) SLMPD has several pieces of hardware and software that are used to investigate crimes, but only in exigent circumstances, after obtaining a court ordered search warrant or consent of the owner or user of the device.
3) Deployment of these technologies is based on a court ordered search warrant signed by a judge.
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?

The investigating officer must obtain the consent of the device owner, obtain a search warrant or exigent circumstances must exist prior to the utilization of these technologies. This search warrant requires the establishment of a probable cause, which are the facts and circumstances that police officers know about, based on reasonably trustworthy information, are sufficient in themselves to warrant a belief by a man of reasonable caution that a crime is being or has been committed.

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

Use of the Saint Louis Metropolitan Police Department Cybercrimes Technologies is strictly limited to the terms outlined in the court issued search warrant. Data extraction/examination forensic technologies shall not be used for personal purposes. The equipment shall not be used for illegal purpose, and shall not be used to harass, intimidate, or discriminate against any individual or group. These technologies must be used in accordance to a court issued search warrant or in exigent circumstances to identify a suspect in an active criminal investigation that could lead to a greater concern for public safety if not identified.

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

To utilize these technologies, exigent circumstances must exist, or investigators must obtain a search warrant to conduct the forensic examination of the devices. Once a search warrant is obtained the investigator must use the technologies in accordance with the terms of the court approved search warrant. The data collected during use of these technologies is used as evidence to further criminal investigations.

DEPLOYMENT:

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.

Cybercrimes technologies are deployed based on exigent circumstances and/or the execution of the court approved search warrants that have been obtained by the investigators.

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.

The total cost for these technologies has been $10,713.33 paid by the Saint Louis Police Foundation. There has also been software recently purchased by the Saint Louis Police Foundation to enhance investigations for cybercrimes. The total cost of that software was $210,000, and that cost will be a yearly cost.

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 includes not deploying until the investigator has exigent circumstances or has obtained a court ordered search warrant related to a criminal investigation, or during their investigation they have obtained the consent of an individual who is the owner of a device that is related to their investigation. These technologies have been utilized 723 times in 2023 and for exigent circumstances a total of 164 times. In 2024, the technologies have been utilized 712 times and 129 times in for exigent circumstances year to date.

The SLMPD is committed to upholding the civil rights and liberties of all citizens. SLMPD complies with SO 1-08, SO 1-04, and directive 2021-08-27.

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 but are not limited to various forms of communications, images, IP Addresses, and application uses. Access to these forms of data is authorized by a court issued search warrant.

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?*

There is no data that is inadvertently collected during the use of the technologies. Technologies can only be accessed in the SLMPD Cybercrimes Unit.

c) *How inadvertently collected surveillance data is be expeditiously identified and deleted?*
There is no data that is inadvertently collected during the use of the technologies.

d) *How the City Entity will ensure that, when it retains surveillance data, such retention will comply with the Missouri Records Retention Schedule?*
The data obtained using the technologies is part of a criminal investigation and is considered evidence of a crime. The retention of the data is determined by the State Retention Schedule related to the crime being investigated. Most of the crimes investigated by the Cybercrimes Unit have no statute of limitation.

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.

Data obtained using the technology is stored as evidence in a secured area of the department with access by only the investigators and forensic analysis assigned to the investigation.

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.

The data obtained using the technologies is part of a criminal investigation and is considered evidence of a crime. The retention of the data is determined by the State Retention Schedule related to the crime being investigated. Most of the crimes investigated by the Cybercrimes Unit have no statute of limitation.

SURVEILLANCE DATA SHARING:

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;*

Only SLMPD investigators assigned to the Cybercrimes Unit doing forensic analysis have access to the technology. Their analysis is after the lead investigator on a case has obtained a court issued search warrant are able to use the technologies for forensic analysis of devices. Unless there is an exigent circumstance which the Cybercrimes Unit will access the data to identify a suspect involved in an active criminal investigation that can lead to a large community public safety concern.

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.

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 unauthorize persons and entities.
Only SLMPD investigators that have exigent circumstances, obtained consent from the owner/user or have obtained a court issued search warrant are able to use the technologies for their criminal investigations.

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.

The data obtained after a court issued search warrant and/or data obtained after exigent circumstances exit, is part of evidence in a criminal case.

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.

There are a limited number of SLMPD investigators who are trained in the use of the technologies. When there is a reassignment of an investigator, training is conducted by an outside entity, dependent on the technology. Mobile data extraction training was last conducted in 2024 for investigators. The technologies are overseen by the Cybercrimes Unit and the commander is responsible for ensuring the proper use of the technologies and compliance with all policies and procedures.

AUDITING AND OVERSIGHT:

What mechanisms will be implemented to ensure the Surveillance Use Plan is followed, included 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?

This technology is overseen by the Cybercrimes Unit in the department. The Commander of the Unit is responsible for ensuring the proper use of the technologies and ensuring compliance with all policies and procedures.

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.