St. Louis Metropolitan Police Department

Surveillance Use Plan

SURVEILLANCE TECHNOLOGY:

Cybercrime Technologies – Magnet GrayKey

DESCRIPTION:

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

The St. Louis Metropolitan Police Department's Cybercrimes Unit utilizes various forensic examination technologies for criminal investigations. The unit utilizes Magnet GrayKey hardware and software to extract cell phone data without altering the data or adding data to the phone. Devices are connected to the GrayKey tool, and the data is extracted from the phone. GrayKey is designed to complete the extraction without altering any of the data or adding data to the phone.

The technology is used to gather evidence for criminal investigations after obtaining a court ordered search warrant or with the written consent of the device's owner or the device's user. This technology is used in exigent circumstances. 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 with 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 St. Louis Metropolitan Police Department utilizes Magnet GrayKey hardware and software to extract cell phone data without altering the data or adding data to the phone. The technology is used to gather evidence for criminal investigations after obtaining a court ordered search warrant or with the written consent of the device's owner or device's user. This technology is used in exigent circumstances.

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 the GrayKey technology to extract cellphone data related to criminal investigations, where a court-ordered search warrant has been granted, or where the owner/user of the device provides written consent, or during exigent circumstances that possesses a threat to the safety of the community.
2) SLMPD has the GrayKey hardware and software tool utilized by the department's Cybercrimes Unit.

3) Deployment of this technology is based on a court-ordered search warrant that has been granted, or with the written consent of the device owner/user, or during exigent circumstances that possesses a threat to the safety of the community.
4) SLMPD does not have any organizational MOUs or partnerships for this technology.

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 written 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.

This technology is also used in exigent circumstances. 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 with identifying a suspect or using the technology to identify the origin of a bomb/school shooting threats.

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 purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group. These technologies must be used in accordance with 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.

The data obtained in the extraction is reviewed and analyzed by investigators assigned to the Cybercrimes Unit, who are trained in the use of the technology. Data extracted from the device is

maintained for the criminal investigation and all data is retained based on the statute of limitations for the associated crime as defined by state laws and the State of Missouri Police Records Retention Schedule.

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. Device owners/users can also provide written consent for access to their device.

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.

GrayKey costs approximately $65,000 annually. The St. Louis Police Foundation has covered the first two years of the technology, and the department will budget for this in the future.

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?

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. Device owners/users can also provide written consent for access to their device.

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).*

DATA COLLECTION:

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

The data obtained from this technology includes the data on a cellphone. GrayKey technology is capable of extracting call logs, text messages, emails, photos, videos, contacts, browsing history,

app data, and location data. GrayKey can also extract data from some social media apps on the phone.

GrayKey software can also analyze deleted data and hidden files on a device and can recover data that has been deleted.

The extracted data is then stored on a secured server located in the Cybercrimes Unit, only accessible to Cybercrimes investigators.

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 this technology. The data obtained in the extraction is reviewed and analyzed by investigators assigned to the Cybercrimes Unit, who are trained in the use of the technology. Since the data extracted from the device is part of a criminal investigation, it is retained based on the statute of limitations for the associated crime as defined by state laws and the State of Missouri Police Records Retention Schedule. The retention of the data is managed by the SLMPD Cybercrimes Unit.

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

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 extracted from the device is part of a criminal investigation, it is retained based on the statute of limitations for the associated crime as defined by state laws and the State of Missouri Police Records Retention Schedule. The retention of the data is managed by the SLMPD Cybercrimes Unit.

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 GrayKey software and equipment are stored and maintained in the Cybercrimes Unit, a secured office within the SLMPD Headquarters. Only authorized users have access to the technology. Each user is required to use a unique login and password to access the software and conduct data extractions.

The software is not accessible by the vendor. Additionally, the software can only be installed through a specific process, it cannot be moved, and the user must be an authorized user with a valid software license. The GrayKey software cannot be accessed outside of the department.

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 extracted from the device is part of a criminal investigation, it is retained based on the statute of limitations for the associated crime as defined by state laws and the State of Missouri Police Records Retention Schedule. The retention of the data is managed by the SLMPD Cybercrimes Unit.

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 who have been trained in the use of the GrayKey technology have access to the technology, which is located in the secured Cybercrimes Unit.

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.

Data that has been extracted using the GrayKey technology is not shared without a court order or other legal proceedings such as discovery. The extracted data is considered confidential, and there is no third-party access or sharing. The vendor does not have access to the extracted data.

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 GrayKey technology. Training is conducted by outside vendors who specialize in the use of the technology. Mobile data extraction training was last conducted in 2024 for investigators and those trained were provided certificates of completion. The technology is 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.

Data is only extracted via legal authority, such as a court ordered search warrant, the owners written consent, or exigent circumstances. Misuse of the system is reported to and investigated by the Bureau of Professional Standards Internal Affairs Unit. Failure to follow departmental policies and procedures, or user agreement terms can result in disciplinary actions and/or criminal proceedings.

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.