St. Louis Metropolitan Police Department

Surveillance Use Plan

SURVEILLANCE TECHNOLOGY:

Cybercrime Technologies – BERLA

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 BERLA iVe ecosystem, which is a collection of tools supporting investigators throughout the vehicle forensic process with a mobile application for identifying vehicles, a hardware kit for acquiring systems, and forensic software for analyzing data.

The iVe Mobile allows investigators to identify vehicles supported by iVe, determine which systems are installed, know what data can be retrieved, and how to acquire the data – all before taking any action. It provides instructions for locating and removing vehicle systems and monitors the progress of long-running acquisitions.

The iVe Toolkit is a collection of specifically developed interface boards and cables used to acquire various supported vehicle systems. The toolkit includes tools to help remove the systems from a vehicle when required. The interface boards and cables are used in conjunction with the iVe software to acquire the data.

iVe Desktop is a Windows based application. It is the workhorse of the iVe ecosystem and is used for all acquisitions. It is used to parse data, recover deleted information and view raw file systems. iVe Desktop includes a full suite of analysis and reporting tools to include mapping, data export, search, and timeline analysis.

The technology is used to gather evidence for criminal investigations after obtaining a court-order search warrant, with the vehicle owner's written consent, or 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 information from a victim's vehicle who was the victim of a deadly crime to assist with obtaining leads in the case.

PURPOSE:

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

The St. Louis Metropolitan Police Department utilizes BERLA to extract and analyze data stored within a vehicle's Infotainment/Telematics System. The data can include vehicle events, location data, and connected devices. The analysis of the vehicle data can help determine what happened, where it happened, and who was involved.

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 BERLA technology to extract vehicle data related to criminal investigations, where a court-ordered search warrant has been granted, with the vehicle owner's written consent, or during exigent circumstances.
2) SLMPD has the BERLA iVe Ecosystem, which is utilized by the department's Cybercrimes Unit.
3) Deployment of this technology is based on a court-ordered search warrant that has been granted, with the vehicle owner's written consent, or during exigent circumstances.
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 vehicle owner, obtain a search warrant or exigent circumstances must exist prior to the utilization of this technology. 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 information from a victim's vehicle, when the person is the victim of a deadly crime.

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. BERLA 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 vehicle. Once a search warrant is obtained the investigator must use the technology 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 vehicle 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. Vehicle owners/users can also provide written consent for access to their vehicle's information.

Additionally, this technology is used after a crime has been committed during the investigation of that crime and the analyzed data is provided to the investigator as part of the investigation follow-up. A request to obtain data is made by the investigator of the incident. The toolkit is used to obtain data from a vehicle, not a person.

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.

BERLA iVe costs approximately $8,000 annually. This cost is included in the department's annual general fund budget.

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. Vehicle owners/users can also provide written consent for access to their vehicle information.

The BERLA technology is used after a crime has been committed during the investigation of that crime and the analyzed data is provided to the investigator as part of the investigation follow-up. A request to obtain data is made by the investigator of the incident. The toolkit is used to obtain data from a vehicle, not a person.

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 vehicle events, location data, and connected devices. The events are events such as door openings, ignition activity, and seatbelt usage. They are recorded along with a date/time stamp and the GPS location of the vehicle at the time of the event. Some location data is included in the vehicle events and others in what are called Track Logs. The software analyzes location data into what it believes are vehicle trips (tracks) to show where the vehicle was located (based on GPS coordinates) at a given date/time. Connected devices show what devices have been paired with the vehicle system. These can include some cellular phone data, such as contacts and call logs. There is a chance a vehicle may contain devices connected to the vehicle that are unrelated to the specific criminal case. When this occurs, the analyzing investigator will need to make this determination and then not further analyze that specific device. This is also restricted by the scope of the search warrant obtained to acquire and analyze the data.

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 a chance a vehicle may contain devices connected to the vehicle that are unrelated to the specific criminal case. When this occurs, the analyzing investigator will need to make this determination and then not further analyze that specific device. This is also restricted by the scope of the search warrant obtained to acquire and analyze the data.

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

The search warrant scope is restrictive to minimize the amount of inadvertently collected information.

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.

Only SLMPD investigators that are authorized and trained in the use of the BERLA technologies are allowed to access the system. Each user is required to use a unique login and password to access the software. The Commander of Cybercrimes approves access to the BERLA iVe ecosystem.

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 vehicles.

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 BERLA iVe technology have access to the technology.

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 BERLA iVe 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 BERLA technology. Investigators must successfully complete a BERLA-certified training course to have "certificed access" or a non-certified training course to have "non-certified" access prior to use. These two distinctions give BERAL a tiered system for access. 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.