St. Louis Metropolitan Police Department

Surveillance Use Plan

SURVEILLANCE TECHNOLOGY:

Saint Louis Mugshot Recognition Technology (SMRT)

DESCRIPTION:

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

The Saint Louis Mugshot Recognition Technology (SMRT) is a digital technology that the department has access to through the department's REJIS subscription and a collaboration with participating agencies through the St. Louis Fusion Center. SMRT is a facial comparison technology that is used by the St. Louis Metropolitan Police Department to compare subject probe images to an arrest photo database for law enforcement purposes. It applies an algorithm to compile an array of photographs with physical characteristics similar to those of the suspect in the submitted photo. SMRT technology does not provide analysis to positively identify individuals. The technology provides investigators with possible leads that require additional investigative steps, under proper legal authority, to follow the leads provided.

Request for use of the SMRT system can be made by contacting the Real-Time Crime Center (RTCC). It should be noted that the RTCC is a part of the St. Louis Metropolitan Police Department and staffed by SLMPD personnel. The RTCC is a hub of surveillance technologies and does not fall under sharing for any surveillance technologies.

It should be noted that the St. Louis Fusion Center is a collaborative effort between agencies in the St. Louis area to reduce crime in the St. Lous region, it is staffed with law enforcement personnel from various law enforcement agencies including the St. Louis Metropolitan Police Department.

PURPOSE:

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

Specifically, absent a final court order requiring or authorizing some different use(s), the shared SMRT data may be used for the following purposes (and in any prosecution(s) resulting from such use):

- The investigation, detection, or analysis of crime;
- The investigation, detection, or analysis of violation of Missouri, and/or Illinois, and/or federal criminal or other public safety law;
- The investigation, detection, or analysis of the operation of one or more terrorist(s);
- The investigation, detection, or analysis of missing or endangered person(s); or
- To enable law enforcement personnel to gain accurate identification verification regarding persons encountered in public safety situations, such as traffic stops, pedestrian interviews, vehicle accidents, workplace injuries, and/or assaults/shooting scenes; lost/found elderly, mentally-disabled, and/or non-communicative persons; and/or children found with adults not their parents/guardians; and/or in contexts when persons seem to have provided, instead of their true

names, entirely false names, partially false names, relatives' names, nicknames, purposeful misspellings of true names, and/or names that have been modified without a court order (such as by adding a self-chosen appendage to a surname).

The above is not an exclusive list of examples of legitimate law enforcement uses of the shared SMRT data. In providing this list, this use plan is not meant to inhibit other legitimate law enforcement use(s) of the SMRT system for any other purpose(s) for which visual examination of booking mugshots traditionally and lawfully occurs.

In no event will access to the SMRT system database be permitted to investigate, analyze, review, or gather information solely concerning any action or speech protected by the First Amendment to the United States Constitution.

In no event will any query or the SMRT system database occur other than by a human initiated query (i.e., automated mass query processes associated with data-mining-type activity will not be permitted).

The collection of mugshot images by project-participating agencies using cameras in any manner known to the collecting agency to solely reflect an individual's political, religious, or social views, associations, or activities (i.e., not as a result of post-arrest booking or any other contact with a law enforcement agency for which mugshot photographs are generally taken) must be limited to instances directly related to criminal conduct or activity which, as standard practice, required an agency to take a mugshot image of a person.

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 SMRT to continue to assist in developing leads in active criminal investigations and to continue assisting in closing cases for victims of crimes.
2) SLMPD currently has access to SMRT through the REJIS subscription.
3) The technology is deployed in active criminal investigations as stated above in the PURPOSE of this use plan.
4) SLMPD has access to this technology through the subscription with REJIS and the system is maintained by the St. Louis Fusion Center.

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

The Saint Louis Mugshot Recognition Technology is governed by SO 5-27, which states the following:

Specifically, absent a final court order requiring or authorizing some different use(s), the shared SMRT data may be used for the following purposes (and in any prosecution(s) resulting from such use):

- The investigation, detection, or analysis of crime;
- The investigation, detection, or analysis of violation of Missouri, and/or Illinois, and/or federal criminal or other public safety law;
- The investigation, detection, or analysis of the operation of one or more terrorist(s);
- The investigation, detection, or analysis of missing or endangered person(s); or
- To enable law enforcement personnel to gain accurate identification verification regarding persons encountered in public safety situations, such as traffic stops, pedestrian interviews, vehicle accidents, workplace injuries, and/or assaults/shooting scenes; lost/found elderly, mentally-disabled, and/or non-communicative persons; and/or children found with adults not their parents/guardians; and/or in contexts when persons seem to have provided, instead of their true names, entirely false names, partially false names, relatives' names, nicknames, purposeful misspellings of true names, and/or names that have been modified without a court order (such as by adding a self-chosen appendage to a surname).

The above is not an exclusive list of examples of legitimate law enforcement uses of the shared SMRT data. In providing this list, this use plan is not meant to inhibit other legitimate law enforcement use(s) of the SMRT system for any other purpose(s) for which visual examination of booking mugshots traditionally and lawfully occurs.

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

SMRT can be accessed by commissioned personnel for law enforcement purposes only.

In no event will access to the SMRT system database be permitted to investigate, analyze, review, or gather information solely concerning any action or speech protected by the First Amendment to the United States Constitution.

In no event will any query or the SMRT system database occur other than by a human initiated query (i.e., automated mass query processes associated with data-mining-type activity will not be permitted).

The collection of mugshot images by project-participating agencies using cameras in any manner known to the collecting agency to solely reflect an individual's political, religious, or social views, associations, or activities (i.e., not as a result of post-arrest booking or any other contact with a law enforcement agency for which mugshot photographs are generally taken) must be limited to instances directly related to criminal conduct or activity which, as standard practice, required an agency to take a mugshot image of a person.

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 are governed by SO 5-27. The St. Louis Fusion Center's authorized personnel will have the ability to query the image database in the system and view the returned image(s), if any, of matches, and view basic booking data associated with the returned image(s). It should be noted that the St. Louis Fusion Center is a collaborative effort between agencies in the St. Louis area to reduce crime in the St. Lous region, it is staffed with law enforcement personnel from each agency including the St. Louis Metropolitan Police Department. Data is also reviewed by the requesting investigating officer or detective to determine if a positive identification can be made from the leads provided by the system for further investigative steps to be taken by the officer/detective.

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.

The use of SMRT is for active criminal investigations and is not used based on geography.

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.

There is no specific cost for this technology as it is part of the REJIS subscription. The subscription for REJIS is $1,835,397.24 annually.

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?

This technology is used during active criminal investigations. A possible facial comparison match is only a lead, requiring additional investigative steps. An arrest is not made until the investigator establishes, with other corroborating evidence, that the suspect identified as a possible match is the perpetrator of the crime being investigated. In all steps of the use of the technology, there is a human component to ensure that the technology is not the sole deciding factor in the photo comparison.

DATA COLLECTION:

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

The data collected is a photo comparison of a probe image (the image of the subject in question) to an array of photographs collected by the law enforcement agencies participating in the SMRT Data Sharing Project. SMRT data includes booking mugshots and associated identifying information routinely accompanying mugshots, such as names, date of births, and any other identifying information collected at the time of an arrest during the booking process.

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?*
This technology is used to compare a static image to a database. There is no data that is inadvertently collected during the authorized use of this technology because the data is being put into a system not collected from the system.

c) *How inadvertently collected surveillance data is be expeditiously identified and deleted?*
There is no inadvertently collected data that is collected by 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?*
All SMRT system data provided to the Saint Louis Fusion Center will be stored on the SMRT server for a period not to exceed ten (10) days after the date that the originating agency for each submitted image notifies the SMRT System Administrator that it no longer retains the mugshot in its records.

Should SMRT system data be determined to have evidentiary value, the following applies:

(1) In those circumstances when data is identified as having evidentiary value, the SMRT System Administrator, or designee, must be notified in writing of that circumstance and, absent receipt of a written retention order from an appropriate authority, will review the facts of the specific case and determine if the data should be saved. If, upon review or upon receipt of a retention order from appropriate authority, the SMRT System Administrator or designee determines it is reasonable to believe the data has evidentiary value, the SMRT System Administrator or designee will authorize the transfer of the applicable data from the SMRT Program server to a form of digital storage media (CD, DVD, etc.) or other portable storage devices.

(2) Agencies requiring data to be retained by the St. Louis Fusion Center beyond the established retention period may make a formal request to the SLFC to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The SLFC may grant or deny agency requests based on the information provided and applicable law.

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 information for the SMRT system is only accessible by commissioned personnel and is accessible only through the REJIS system. The REJIS system is only accessible through a unique login for each law enforcement agency user who has completed the training provided by REJIS for use of the system.

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.

All SMRT system data provided to the Saint Louis Fusion Center will be stored on the SMRT server for a period not to exceed ten (10) days after the date that the originating agency for each submitted image notifies the SMRT System Administrator that it no longer retains the mugshot in its records.

Should SMRT system data be determined to have evidentiary value, the following applies:

(1) In those circumstances when data is identified as having evidentiary value, the SMRT System Administrator, or designee, must be notified in writing of that circumstance and, absent receipt of a written retention order from an appropriate authority, will review the facts of the specific case and determine if the data should be saved. If, upon review or upon receipt of a retention order from appropriate authority, the SMRT System Administrator or designee determines it is reasonable to believe the data has evidentiary value, the SMRT System Administrator or designee will authorize the transfer of the applicable data from the SMRT Program server to a form of digital storage media (CD, DVD, etc.) or other portable storage devices.

(2) Agencies requiring data to be retained by the St. Louis Fusion Center beyond the established retention period may make a formal request to the SLFC to extend retention. Each request must specify the need for extended retention, the circumstances surrounding the request, the requesting agency's case number, and a specific point of contact within the requesting agency. The SLFC may grant or deny agency requests based on the information provided and applicable law.

SLMPDs retention of evidentiary data is determined by the classification of the type of incident per the State of Missouri's Police Records Retention Schedule.

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;*
All commissioned law enforcement personnel at participating agencies, who have access through REJIS, have access to information provided to the St. Louis Fusion Center via the SMRT system.

b) How much sharing is necessary for the stated purpose and use of the surveillance technology;
SMRT data is provided to the St. Louis Fusion Center and is used as part of the SMRT database for photo comparison by participating agencies in the region.

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.
Access to the SMRT system is through a REJIS subscription. REJIS follows the federal laws related to Criminal Justice Information Systems and thus any commissioned personnel in a law enforcement agency must be in compliance with those laws or disciplinary or criminal actions will be taken.

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.

Access to the SMRT system is through a REJIS subscription. REJIS follows the federal laws related to Criminal Justice Information Systems and thus any commissioned personnel in a law enforcement agency must follow those laws or disciplinary or criminal actions will be taken. Individuals that are not cleared to have CJIS access are unauthorized to have access to REJIS or any other information/technologies provided by REJIS.

Should SMRT system data be determined to have evidentiary value, the following applies the SMRT System Administrator, or designee, must be notified in writing of that circumstance and, absent receipt of a written retention order from an appropriate authority, will review the facts of the specific case and determine if the data should be saved. If, upon review or upon receipt of a retention order from appropriate authority, the SMRT System Administrator or designee determines it is reasonable to believe the data has evidentiary value, the SMRT System Administrator or designee will authorize the transfer of the applicable data from the SMRT Program server to a form of digital storage media (CD, DVD, etc.) or other portable storage devices.

SLMPDs retention of evidentiary data is determined by the classification of the type of incident per the State of Missouri's Police Records Retention Schedule.

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.

The information for the SMRT system is only accessible by commissioned personnel and is accessible only through the REJIS system. The REJIS system is only accessible through a unique login for each law enforcement agency user who has completed the training provided by REJIS for use of the system.

REJIS follows the federal laws related to Criminal Justice Information Systems (CJIS) and thus any commissioned personnel in a law enforcement agency must follow those laws or disciplinary or criminal actions will be taken. Individuals that are not cleared to have CJIS access are unauthorized to have access to REJIS or any other information/technologies provided by REJIS.

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?

All transactions and queries of the SMRT Server system are logged, immutably, and are subject to review at any time. Anyone found to misuse the system is subject to disciplinary actions, up to and including criminal prosecution.

In order to facilitate the periodic and random audits necessary to monitor user compliance with laws and policies, audit logs will include certain information. Specifically, queries to the SMRT Server will be immutably logged and include:

- The identity and purpose of the user initiating the query.
- The prove image element used to query the SMRT system (however, the prove image will not be enrolled in the system for further searchers, but is retained only as an audit-enabling feature);
- Valid reason for the search; and
- Date and time of the inquiry.

Primary responsibility for ensuring compliance with the provisions of Special Order 5-27 is assigned to the Commander of the Real-Time Crime Center. The Commander of the RTCC will designate a SMRT System Administrator, who will be responsible for the overall management of the SMRT program. Both the Commander of the RTCC and the SMRT System Administrator will be responsible for making SMRT system reports available to the public, as well as or ensuring that Special Order 5-27 is both available to the public and, as may be needed is updated.

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.