

**METROPOLITAN POLICE DEPARTMENT – CITY OF ST. LOUIS
OFFICE OF THE POLICE COMMISSIONER
SPECIAL ORDER**

Date Issued: April 19, 2016 **Order No.:** Section V of SO 5-27
Effective Date: April 19, 2016 **Expiration:** Indefinite

Reference:

CALEA Standards:

Cancelled Publications:

Subject: ST. LOUIS MUGSHOT RECOGNITION TECHNOLOGY (SMRT)

To: ALL BUREAUS, DISTRICTS AND DIVISIONS

PURPOSE: To establish guidelines and principles for the collection, analysis, use, dissemination, retention, and destruction of information (also known as data) regarding the St. Louis Mugshot Recognition Technology's (SMRT) operations.

POLICY: SLMPD will comply with all applicable laws and regulations as they pertain to the collection, analysis, use, dissemination, retention, and destruction of data obtained through its St. Louis Mugshot Recognition Technology (SMRT) system. The SLMPD will utilize and share information with the St. Louis Fusion Center (SLFC), and [REDACTED]

A. GENERAL INFORMATION

1. The SMRT Server system, managed by SLFC, provides the database, query tool, history tracking, and reporting for the SMRT program. It manages and provides a temporary storage and search structure for the probe image information being collected in the field. It does not provide analytic search-capable storage of that in-the-field-created information beyond its comparison, as a probe image, to stored mugshots. [REDACTED]

2. The SMRT system does not use facial recognition analysis to positively identify individuals. Rather, the technology applies an algorithm to compile an array of photographs with physical characteristics similar to those of the suspect in the submitted photo. Investigators may then take the logical investigative steps, under proper legal authority, to generate and pursue leads based upon the results.

3. [REDACTED] SLFC-authorized personnel will have the ability to:

- a. Query the image database in the system and view the returned image(s), if any, of matches; and

SO 5-27

- b. View basic booking data associated with the returned image(s).

B. USING SMRT

1. 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):
 - a. the investigation, detection, or analysis of crime;
 - b. the investigation, detection, or analysis of violation of Missouri, and/or Illinois, and/or federal criminal or other public safety law;
 - c. the investigation, detection, or analysis of the operation of one or more terrorist(s);
 - d. the investigation, detection, or analysis of missing or endangered person(s); or
 - e. 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 assault/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).
2. The above are non-exclusive examples of legitimate law enforcement uses of the shared SMRT data. In providing this list, this policy 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.
3. 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.
4. In no event will any query of 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).
5. 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. SMRT INQUIRIES

1. Detectives or Officers can request the use of SMRT by contacting the Real-Time Crime Center (RTCC).

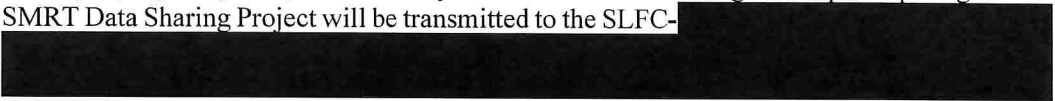
SO 5-27

2. Detectives or Officers must identify the reason of the request, complaint number, or any other possible identifier or information regarding the request.
3. SMRT requires the highest quality image able to be obtained.
 - a. Large digital images/files may require delivery of a CD, DVD, or other storage device with the image to the RTCC.
 - b. Investigators can also provide information to the RTCC regarding the source from which the image was obtained.
4. The RTCC will generate a Facial Recognition Image Compare Report.

NOTE: Identity comparisons with SMRT are nonscientific and are intended for investigative lead purposes only. These investigative leads should not be used as the sole basis for any decision in the investigation. The intent of this SMRT analysis is only to illustrate facial similarities or differences between two subjects – not to make a positive identification.

5. In the event that the information provided by the RTCC in the Facial Recognition Image Compare Report is used to make a positive identification, the Facial Recognition Image Compare Report will be seized as evidence and handled in accordance with Department policy.
6. Detectives or Officers will fully document the use of any positive identification that was made with the assistance of the SMRT system in the I/Leads report.

D. DATA COLLECTION, RETENTION, AND DISEMINATION

1. SMRT data (i.e., booking mugshots and associated identifying information routinely accompanying mugshots) collected by the law enforcement agencies participating in the SMRT Data Sharing Project will be transmitted to the SLFC-


3. All SMRT system data provided to the SLFC 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.

4. Should SMRT system data be determined to have evidentiary value, the following applies:
 - a. 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 an appropriate authority, the

SO 5-27

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.

- b. Agencies requiring data to be retained by the SLFC 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.

E. AUDIT LOGS

1. 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 action, up to and including criminal prosecution.
2. 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:
 - a. The identity and purpose of the user initiating the query;
 - b. The probe image element used to query the SMRT system (however, the probe image will not be enrolled in the system for future searches, but is retained only as an audit-enabling feature);
 - c. Valid reason for the search; and
 - d. Date and time of the inquiry.

F. RESPONSIBILITIES

1. Primary responsibility for ensuring compliance with the provisions of this policy is assigned to the Commander of the RTCC.
2. The Commander of the Real-Time Crime Center will designate an SMRT System Administrator, who will be responsible for the overall management of the SMRT Program.
3. 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 for ensuring that this SO document is both available to the public and, as may be needed, is updated.