Santa Clara County Office of the Sheriff

Surveillance Use Policy for Facial Recognition Software

1. Purpose

The purpose of Facial Recognition Software shall be to assist law enforcement in the identification of persons involved in a criminal investigation. A criminal investigation is an official investigation regarding a suspected violation of law.

Facial Recognition Software shall work by scanning a static photograph and comparing it to a law enforcement mugshot arrestee database or other lawfully accessed database in order to locate a possible match. Although a search warrant is generally not required to utilize facial recognition software, a search warrant shall be obtained if it is legally required.

The Santa Clara County Sheriff's Office recognizes that Facial Recognition Software is only one investigative step and the results shall not be exclusively relied upon to provide a sole, definitive identification of an individual. The Sheriff's Office utilizes Walnut Creek, CA based Forensic Logic Inc. facial recognition software. This Facial Recognition Software shall be a tool that may be utilized in conjunction with other investigative steps during a criminal investigation to identify individuals associated with a criminal investigation.

2. Authorized and Prohibited Uses

Sheriff's personnel shall only utilize Facial Recognition Software during a criminal investigation to assist in the identification of unknown persons associated with a specific criminal investigation.

Facial Recognition Software shall only be utilized for official law enforcement purposes to assist in a specific criminal investigation.

Access to Facial Recognition Software shall be limited to Sheriff's Office personnel involved in a specific criminal investigation, including oversight by supervisors or administrative command staff; and to other law enforcement agencies if approved by the Sheriff or designee for a specific criminal investigation. In all instances, access to the software shall require security identification, password authentication, and incident number documentation.

Facial recognition software shall only be used to compare static photographs to a law enforcement database or other lawfully accessed database and shall not be used in combination with or integrated into any other technology.

Facial Recognition Software shall not be used for personal or non-law-enforcement purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group.

3. Data Collection

Facial Recognition Software shall analyze and compare submitted static images with known images (e.g., from the County's arrestee mugshot database) and provide the user with potential matches.

4. Data Access

Access to data results from Facial Recognition Software shall be limited to Sheriff's Office personnel engaged in a specific criminal or administrative investigation, including supervisors and administrators; and to other county personnel designated in writing by the Sheriff or the Sheriff's designee if they determine that access is reasonably necessary for a County business reason, which may include a specific criminal, civil, or administrative investigation or action.

5. Data Protection

Sheriff's personnel shall only have access to Facial Recognition Software on approved Sheriff's Office computers or secured networks, which require a secure log-in and an authenticated password. Access to the software shall require security identification, password authentication, and incident number documentation.

6. Data Retention

Results for potential matches shall be printed or saved only for the purposes of documentation or evidence in an investigation and shall be maintained and retained in accordance with applicable state or federal evidentiary laws and Sheriff's Office policy. Results stored in the system shall be deleted from the system no longer than 180 days from the initial query.

7. Public Access

Data from Facial Recognition Software shall be made public or deemed exempt from public disclosure pursuant to state or federal law. For public requests for data, the Sheriff's Office shall confer with County Counsel to determine whether the requested data is exempt from disclosure pursuant to the California Public Records Act, or is legally required to be disclosed, and shall respond to requests in compliance with applicable law.

8. Third-Party Data-Sharing

It shall be permissible for data from Facial Recognition Software to be shared with only the following:

- District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;
- Public Defender's Office or criminal defense attorney via the District Attorney's Office in according with California discovery laws;

- Other law enforcement offices as part of a specific criminal or administrative investigation;
- Parties in a civil litigation involving the County, in response to a subpoena or civil discovery;
- County Personnel Board, arbitrator, or Court regarding a county administrative action or litigation;
- Other third parties, pursuant to a Court Order.

9. Training

Training for the use of the Facial Recognition Software shall be provided by Sheriff's Office personnel or the vendor for authorized users. Sheriff's personnel utilizing Facial Recognition Software shall be provided a copy of this Surveillance Use Policy.

10. Oversight

Division Commanders of divisions utilizing facial recognition software shall ensure compliance with this Surveillance Use Policy. Sheriff's Administration shall conduct periodic audits as it deems necessary, and at least annually, of data access to ensure policy compliance.

Approved as to Form and Legality

11/19/18

Rob Coelho
Office of the County Counsel