Santa Clara County Office of the Sheriff

Surveillance Use Policy for the City of Saratoga's Automated License Plate Readers

1. Purpose

Automated license plate readers (ALPRs) use high speed cameras to photograph vehicle license plates. The Office of the Sheriff's purpose for using ALPR Technology is to assist the Sheriff's Office in implementing a strategy to assist in criminal investigations, protect residents, and deter crime.

Under the Sheriff's Office's contract to provide law enforcement services to the City of Saratoga (City) and pursuant to a specific, Board-approved agreement between the City and the Sheriff's Office governing ALPRs, it shall be permissible for the Sheriff's Office to manage and/or operate the City's Flock Safety Falcon ALPR (Flock Safety ALPR). To the extent managed and/or operated by the Sheriff's Office, the Flock Safety ALPR shall only be placed at fixed locations for the authorized law enforcement and public safety purposes set forth in this Surveillance Use Policy.

The Flock Safety ALPR may collect license plate information from vehicles on roadways, on property accessible to the public, and on private property. ALPR cameras shall not be installed with the specific purpose of monitoring vehicles on private property. When an ALPR camera is installed, reasonable efforts shall be made to reduce the amount of incidental monitoring of vehicles on private property. A search warrant shall be obtained when legally required.

2. Authorized and Prohibited Uses

With Board approval of a specific agreement, it shall be permissible for the Sheriff's Office to manage and/or operate the Flock Safety ALPR for the City. The Flock Safety ALPR shall only be attached to fixed locations.

The Flock Safety ALPR shall be used for only the following purposes, consistent with Section 1 of this Surveillance Use Policy:

- To locate stolen, wanted, and/or other vehicles that are the subject of specific investigation;
- To locate and/or apprehend individuals subject to arrest warrants or who are otherwise lawfully sought by law enforcement;
- To locate victims, witnesses, suspects, and others associated with a specific law enforcement investigation;
- To locate missing children, adults, and/or elderly individuals, including in response to Amber Alerts and Silver Alerts;

- To support local, state, federal, and regional public safety departments in the identification of vehicles associated with targets of specific criminal investigations, including specific investigations of serial crimes;
- To protect critical infrastructure sites.

Any data obtained from the Flock Safety ALPR shall be used and handled pursuant to this Surveillance Use Policy and applicable state and federal law.

All other uses not referenced above shall be prohibited. The Flock Safety ALPR shall not be used to unlawfully invade the privacy of individuals. Neither the Flock Safety ALPR nor its data shall be used for personal, non-law-enforcement-related purposes; and they shall not be used to harass, intimidate, or discriminate against any individual or group.

3. Data Collection

Digital images of vehicle license plates and their associated license plate numbers shall be collected by the Flock Safety ALPR. The Flock Safety ALPR shall collect the date and time that the license plate passes a digital-image site where an ALPR is located, as well as a captured vehicle's geographical location and vehicle details (make, model, type and color). Live video, vehicle speeds, and audio shall not be provided or recorded.

4. Data Access

It shall be permissible for data collected by the Flock Safety ALPR to be accessible by Sheriff's personnel. Such data shall not be made available through the South Bay Information Sharing System (SBISS).

It shall be permissible for technical and customer support staff from vendors, such as Flock, to access the Flock System ALPR for maintenance and repair of ALPRs on an as-needed basis, and such vendors shall only be tasked with the inspection, troubleshooting, and maintenance of the ALPR system hardware and software configuration, associated cloud storage mechanism and server, as necessary. Vendors shall not be authorized to access specific data collected by ALPRs under any circumstances.

5. Data Protection

The Flock Safety ALPR data shall be stored in a secured cloud environment. Flock Safety ALPR shall maintain multiple layers of physical security and security protection or utilize a cloud service compliant with Criminal Justice Information Services requirements. Encryption for data at rest and in transit, firewalls, authentication, and other reasonable security measures, including the following, shall be utilized to protect ALPR data:

- All ALPR data downloaded to the mobile workstation or in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date, and time.

- Only those employees of the Sheriff's Office working in an investigative or enforcement function shall access ALPR data, and that access shall be only for a purpose authorized in this Surveillance Use Policy.

6. Data Retention

ALPR data from the Flock Safety ALPR associated with a specific criminal investigation may be downloaded onto an electronic storage device or printed. Downloaded, copied, and printed data shall be maintained in accordance with applicable state and federal evidentiary laws, to include retaining the data through the adjudication of a case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations. Flock Safety ALPR data collected by stationary systems shall be purged no later than 30 days from the date it was collected unless the data is needed for a specific investigation. Under those circumstances, the data shall be retained for the duration of the specific criminal investigation and the criminal proceedings through adjudication of the case or in accordance with local, state, and federal court orders or laws governing its use. Data that is flagged by the Flock Safety ALPR, or otherwise downloaded and stored pursuant to this section shall be purged no later than six months from the date it was flagged or downloaded for local storage, unless the data is associated with a specific criminal investigation or an ongoing case for an authorized purpose identified in Section 2 above.

7. Public Access

Flock Safety ALPR data 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 (CPRA), or is legally required to be disclosed, and shall respond to requests in compliance with applicable law. CPRA requests to the County for data from the Flock Safety ALPR shall follow this same review process, but with the inclusion of the City Attorney's Office.

8. Third-Party Data-Sharing

Data from the Flock Safety ALPR may be shared with 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 accordance with California discovery laws;
- Other law enforcement offices as part of a specific criminal or administrative investigation; and
- Parties to civil litigation, in response to a court order.

The City shall delegate any administrative account for the Flock Safety ALPR to the Sheriff's Office and shall not have direct access to data collected and stored by the Flock Safety ALPR. However, it shall be permissible to provide the City with City-owned data

produced by the Flock Safety ALPR, within any parameters set forth in the Board-approved agreement between the Sheriff's Office and the City.

Additionally, it shall be permissible for data to be shared with law enforcement agencies and County-retained investigative personnel to assist with the identification, assessment, investigation, reporting, and prosecution of specific behavior or specific activity that legitimately appears to be: in violation of Department or County rule, policy, or reasonable expectation; illegal; or in furtherance of illegal activity.

Notwithstanding the parties identified above, no data shall be shared in a manner that contradicts Board Policy 3.54 – Cooperation with U.S. Immigration and Customs Enforcement.

9. Training

Training for the operation of the Flock Safety ALPR utilized by the Sheriff's Office shall be provided to all Sheriff's Office personnel who manage or use ALPRs. All Sheriff's Office employees who utilize ALPR Technology shall be provided a copy of this Surveillance Use Policy.

10. Oversight

Sheriff's Administration shall ensure compliance with this Surveillance Use Policy.

All access to and sharing of ALPR data obtained through the Flock ALPR System shall be logged, and the Sheriff's Office shall maintain an audit trail of requested and accessed information, including the purpose of the search. Periodic, random audits shall be conducted by the Sheriff's Office on at least an annual basis. Audits shall ensure compliance with this policy and all applicable laws.

Audit reports shall contain the following information:

- Date and time of access;
- Reason for accessing data;
- Name of law enforcement agency accessing data;
- Activity executed, including any license plate numbers searched; and
- Incident number associated with the investigation.

Required yearly audit reports shall include the name of an agency(s) seeking ALPR data for the purpose of a specific criminal or administrative investigation as well as the frequency of such request. Information shall be presented in a manner that protects the integrity of the request, information, and investigation.

It shall be permissible for audit reports to be shared with government agencies responsible for the costs of those systems requesting more frequent audits, including the City with

respect to the Flock Safety ALPRs. Audit reports for the Flock Safety ALPRs shall be provided to the City Manager within five (5) business days of completion or within the time frame decided pursuant to other mutually agreed upon arrangement. Audits shall be in a format that maintains the confidentiality of the data.

Approved as to Form and Legality

Sam Cretcher 1-28-22

Sam Cretcher
Office of the County Counsel