Automated License Plate Recognition (ALPR) “End-User” Policy

Authorized Purpose for Accessing and Using ALPR Information

The Santa Clara County District Attorney’s Office (SCCDA) is an automated license plate recognition (ALPR) “end-user.” As an “end-user,” authorized personnel employed by the SCCDA access license plate information from systems controlled by private and outside law enforcement ALPR operator agencies to investigate and prosecute criminal activity in Santa Clara County. To support the mission of the SCCDA, authorized SCCDA personnel with a need and right to know will access ALPR data for the following purposes:

- Locate stolen, wanted, and subject of investigation vehicles;
- Locate and apprehend individuals subject to arrest warrants or otherwise lawfully sought by law enforcement;
- Locate victims and witnesses of crime;
- Locate missing or abducted children and elderly individuals, including responding to Amber or Silver Alerts;
- Support local, state, federal and tribal public safety departments in the identification of vehicles associated with targets of criminal investigations, including investigations of serial crimes;
- Protect participants at special events; and
- Protect critical infrastructure sites.

Authorized Users of ALPR Information

The following SCCDA personnel involved in the investigation and prosecution of crime are authorized to access and use ALPR information:

- District Attorney
- Chief Assistant District Attorney
- Assistant District Attorneys
- Deputy District Attorneys
- District Attorney Investigators
- District Attorney Analysts
- District Attorney Paralegals
- Legal Process Officers

Restrictions on use of ALPR Systems

Automated license plate reader data reviewed by an authorized “end-user” may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

SCCDA ALPR “end-users” may not contact occupants of stolen, wanted, or subject-of-investigation vehicles unless the “end-users” are law enforcement officers. SCCDA ALPR law enforcement “end-users” shall follow the SCCDA rules and regulations regarding equipment, protection, self-identification, and use of force when stopping vehicles or making contact.

SCCDA ALPR “end-users” must recognize that the data collected from ALPR devices, and any content-referenced hotlists, consist of data that may or may not be accurate, despite ongoing efforts to maximize the currency and accuracy of such data. To the greatest extent possible, before SCCDA law enforcement personnel contact a subject they will verify and confirm vehicle and subject information using separate law enforcement information sources. SCCDA law enforcement personnel relying on ALPR data must, to the fullest extent possible, visually confirm that the plate characters generated by the ALPR readers correspond with the digital images of the license plate in question.

All SCCDA personnel accessing ALPR data as “end users” are required to acknowledge that they have previously read and understood the SCCDA policy.

In no case shall an ALPR system or data derived from such a system be used for any purpose other than legitimate law enforcement or public safety purposes.

Training

SCCDA provides staff training on the secure handling of confidential and personal information, including ALPR data. The training addresses appropriate handling and transmission procedures, as well as consequences of a security breach.

Only SCCDA staff trained in the use of the ALPR data systems, including its privacy and civil liberties protections, shall be allowed access to ALPR data. Training shall consist of:

- Legal authorities, developments, and issues involving the use of ALPR data and technology;
- Current SCCDA policy regarding appropriate use of ALPR systems;
- Evolution of ALPR and related technologies, including new capabilities and associated risks;
- Technical, physical, administrative, and procedural measures to protect the security of ALPR data against unauthorized access or use;
- Recognition of information technology security incidents, procedures for information technology security incident response, and information security reporting requirements; and
- Practical exercises in the use of ALPR systems.

Training shall be updated as technological, legal, and other changes that affect the use of ALPR systems occur.

ALPR Information Security

Physical and information systems access is limited to SCCDA staff in good standing, who have successfully completed CJIS-compliant background investigations and possess an active physical and/or information systems security clearance.

The County of Santa Clara and SCCDA utilize physical access controls, application permission controls, and other technological, administrative, procedural, operational, and personnel security measures to protect ALPR information from unauthorized access, destruction, use, modification or disclosure.

Audit

Access to, and use of, ALPR data is logged for audit purposes. Audit reports will be structured in a format that is understandable and useful and will contain, at a minimum:

- The name of the authorized user;
- The name of the agency employing the user;
- The date and time of access;
- The activities executed, including any license plates searched for;
- The supplied authorized law enforcement or public safety justification for access; and
- A case number associated with the investigation effort generating the ALPR data query.

At least once during each calendar year, SCCDA will audit a sampling of the ALPR system utilization from the prior 12-month period to verify proper use in accordance with the above-authorized uses. Any discovered intentional misconduct will lead to further investigation, termination of system access, and notification of the user's immediate supervisor for appropriate recourse. In addition, the auditing data will be used to identify systemic issues, inadvertent misuse, and requirements policy changes, training enhancements, or additional oversight mechanisms. The ALPR audits shall be conducted by a SCCDA Project Manager other than the person assigned to manage the SCCDA ALPR function. Audit results shall then be reported to the District Attorney.

ALPR Information Sharing Restrictions

SCCDA only shares ALPR information with authorized law enforcement partners for public safety purposes. Additionally, pursuant to Penal Code section 1054 et seq. and *Brady v. Maryland*, the SCCDA provides ALPR information as criminal discovery to the appropriate defense or appellate attorney of record. SCCDA does not share ALPR information with commercial or other private entities or individuals.

Official Custodian

The Assistant District Attorney of the SCCDA Narcotics Unit is the custodian for implementing the SCCDA ALPR policy.

Accuracy of ALPR Information

In the event that an ALPR operator informs SCCDA of an error associated with ALPR information accessed by SCCDA, SCCDA will correct all associated files. Should SCCDA become aware of an ALPR error, it will correct all associated files and contact the operator that provided the information regarding the error.

ALPR Data Retention

In accordance with the SCCDA Record Retention and Destruction Policy, ALPR data will be stored according to the following schedule:

Case Type	Official Retention Period
Homicide Case Files	Permanent
All Non-Homicide Case Files, Unless Otherwise Stated in this Schedule	Seventy-five years. Case files will be scanned and electronically archived and retained for 75 years. Originals will be retained for a period of at least 90 days to allow scanning for authentication by the department, after which they will be destroyed. Backed up by DA IT provider.
Juvenile Ward Files	When a minor turns 18 and petitions the court for records to be sealed, the record will be destroyed at age 20 or as otherwise ordered by a court of competent jurisdiction. Otherwise as covered by this schedule.
Developmentally Disabled (DD) Case Files	Life of the client.
Plea of Insanity (PC 1026) Case Files	Life of the client.
Juvenile Case Files	Two years after final disposition or until minor attains age of 21, whichever is later. Caveat 1): If cased is appealed, the file must be retained until the final appellate decision is received. Caveat 2): Cases that may be charged as "strikes" should be retained for 75 years.
Certificates of Rehabilitation Case Files	Two years.
Advise and Assist Case Files	Two years.
Expungement Case Files	Two years.
Post-Conviction Proceedings and Special Project Files	Two years.