County of Santa Clara
Office of the District Attorney Surveillance Use Policy

Global Positioning System (GPS) Trackers

1. Purpose

Global Positioning System (GPS) trackers are designed to track the movements and precise location of vehicles, cargo, machinery, and/or individuals.[1] GPS trackers owned by the Santa Clara County District Attorney's Office (SCCDA) shall track only travel speed and/or location data for the object to which it is attached. If the SCCDA seeks to acquire GPS trackers with material surveillance enhancements and/or to use for a purpose, in a manner, or in a location not approved by the Board in this Policy, the SCCDA shall return to the Board for review and/or approval, as applicable, of an updated Surveillance Use Policy, in compliance with the County's Surveillance-Technology and Community-Safety Ordinance.

2. Authorized and Prohibited Uses

Use of GPS trackers shall be limited to only SCCDA personnel authorized by SCCDA Administration to deploy the devices in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA. GPS trackers shall only be utilized pursuant to judicial authorization; with valid consent; or in circumstances that do not violate the Fourth Amendment to the United States Constitution. When the use of a GPS tracker requires a search warrant, the assigned investigator and/or prosecutor shall make an application to the court and obtain court approval before deploying the device. In cases where the use of a GPS tracker is not governed by a search warrant or other court order, the user shall abide by this Surveillance Use Policy.

County-owned GPS trackers and associated data shall not be used for personal, non-SCCDA purposes. The GPS trackers shall not be used for illegal purposes, and shall not be used to harass, intimidate, or discriminate against any individual or group.

3. Data Collection

GPS trackers shall only transmit encrypted data (i.e., movement tracking and location data), which allows authorized personnel in the SCCDA to monitor the device's location in real time. The SCCDA currently has up to six months to download the encrypted location data from the GPS storage company's server via a web application. Judicial authorization may be legally required to obtain data beyond the six-month window. Downloaded data shall be retained in the case file or case/content management system.

//

[1] To promote officer safety and maximize the benefits to be derived from the use of GPS devices, the specific make and model of the GPS devices owned by the SCCDA have been omitted from this Surveillance Use Policy.

4. Data Access

GPS trackers shall be stored in a secure location, and all access and use of the trackers shall be documented in an activity log. The data collected by GPS trackers shall be stored in the physical case file and/or stored within an SCCDA-approved electronic case/content management system. Approved case/content management systems shall log user name, date/timestamp, files or data accessed, and attempts at altering or deleting files.

Access to GPS tracking data shall be limited to only SCCDA personnel authorized by SCCDA Administration to utilize the data in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA, as well as other county personnel designated in writing by the District Attorney or the District Attorney's written designee to the extent that access is necessary for a specific criminal, civil, or administrative investigation or action. The company licensing the GPS trackers has access to only encrypted data (which does not reveal the identity of the subject being tracked), both in transit and at rest.

5. Data Protection

See Section 4 of this Policy. The data from GPS trackers shall be encrypted from the vendor. Credentials including login and password shall be required for authorized personnel to access the GPS tracker data from the system. The County of Santa Clara and the SCCDA shall utilize physical access controls, application permission controls, and other technological, administrative, procedural, operational, and personnel security measures to protect data collected by GPS trackers from unauthorized access, destruction, use, modification or disclosure.

6. Data Retention

Data recovered through the use of GPS trackers, whether downloaded, copied or printed, shall be maintained in accordance with this Surveillance Use Policy, applicable state and federal evidentiary laws, and the SCCDA Record Retention and Destruction Policy approved by the Board of Supervisors on June 21, 2016, as follows:

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.

Case Type	Official Retention Period
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 defendant.
Plea of Insanity (PC 1026) Case Files	Life of the defendant.
Juvenile Case Files	Two years after final disposition or until minor attains age of 21, whichever is later. Caveat 1): If case 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.

Data that is relevant to administrative/personnel-related matters shall be downloaded or otherwise copied, and retained through the adjudication of any administrative, civil, or criminal case in a recognized court of law, as well as allotment of time for an appeals process and statute of limitations; to the extent that data is not covered in the chart above, the data shall be destroyed no later than two years after the later of (1) the time for an appeals process expires; (2) the statute of limitations expires; and (3) for data regarding a County employee's administrative investigation, the date the employee's employment for the County terminates.

All data not downloaded onto an electronic storage device shall be purged from the GPS tracker no later than 90 days from the original recording.

//

7. Public Access

Absent a court order, the public shall not have direct access to data collected by GPS trackers. If a California Public Records Act request, subpoena, or court order is issued for this data, it shall be made public or deemed exempt from public disclosure pursuant to state or federal law, after consultation with the Office of the County Counsel as needed.

8. Third-Party Data-Sharing

The sharing of data recovered through the use of GPS trackers shall be limited to the following third parties:

- Law enforcement agencies when relevant to an ongoing specific investigation or prosecution;
- Defense and appellate counsel and pro se litigants pursuant to Penal Code section 1054 et seq. and *Brady v. Maryland*;
- Individuals who have obtained a valid Court Order, subpoena, or otherwise approved in writing by the District Attorney or written designee.

9. Training

SCCDA shall provide staff with a copy of this Surveillance Use Policy when training on the secure handling of confidential and personal information, including data collected by GPS trackers. The training shall address appropriate handling and transmission procedures, as well as consequences of misuse of the data and a security breach.

10. Oversight

District Attorney's Office Administration shall ensure compliance with this Surveillance Use Policy and all applicable laws. The GPS tracker system shall employ an audit feature, and SCCDA Administration shall conduct audits of the system as it deems necessary, and at least annually, to ensure appropriate use of the system. Sanctions for violation of this Surveillance Use Policy or applicable laws may range from counseling to termination, and in more serious breaches, may result in criminal prosecution.

Approved as to Form and Legality

6/15/2020

Rob Coelho
Office of the County Counsel