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

Third-Party Surveillance Technology

1. Purpose

Law enforcement agencies at the federal, state, and local levels own and utilize various forms of surveillance technology, such as cell-site simulators, license plate readers, GPS trackers, and wiretapping.[1] The agencies use the surveillance technology to document activity and conversations that may be relevant to an ongoing investigation or prosecution. Private third-party entities may also utilize surveillance technology.

For purposes of this Surveillance Use Policy, "**third-party surveillance technology**" means surveillance technology *in the possession, custody, or control of the Santa Clara County District Attorney's Office (SCCDA)* that is not owned, rented, or leased by either Santa Clara County or the SCCDA (i.e., surveillance technologies that are owned by third parties). This Policy provides direction regarding how only that third-party surveillance technology shall be used.

This Policy does not regulate how third parties use their own technology or how they use technology that is not in the possession, custody, or control of the SCCDA. This Policy also does not regulate data that third parties provide to the SCCDA.

2. Authorized and Prohibited Uses

Use of third-party surveillance technology shall be limited to only SCCDA personnel authorized by SCCDA Administration to use the third-party surveillance technology in the course and scope of their employment to support the administrative, investigatory, and prosecutorial functions of the SCCDA. This third-party surveillance technology shall only be used pursuant to judicial authorization; with valid consent of the owner of the technology, and of the subject if the subject's consent is legally required; or in circumstances that, under the law, do not violate anyone's reasonable expectation of privacy.[2] If the use of third-party surveillance technology requires judicial authorization, the assigned investigator and/or prosecutor shall make an application to the court and obtain court approval before deploying the device. In cases where

---

[1] To promote officer safety and maximize the benefits to be derived from the use of third-party surveillance technology, the specific make and model of the devices owned by non-county entities that may be used by authorized personnel in the SCCDA have been omitted from this Surveillance Use Policy.

[2] The Fourth Amendment to the United States Constitution guarantees that people will be safe from unreasonable searches and seizures. A "search" occurs for purposes of the Fourth Amendment when the Government invades a person's "reasonable expectation of privacy." People may have reasonable expectations of privacy in their own person, house, vehicles, and business offices, particularly with respect to things that are not in public view. They also may have a reasonable expectation of privacy in the content of their personal communications such as telephone calls, letters, and journals. In contrast, people have no reasonable expectation of privacy in things they knowingly expose to the public or hold out to public view.

the use of third-party surveillance technology is not governed by a search warrant or other court order, the user shall abide by this Surveillance Use Policy.

Third-party surveillance technology and associated data obtained by the SCCDA shall not be used for personal, non-SCCDA purposes. Third-party surveillance technology and its data 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

Third-party surveillance technology shall typically be used to document a subject's activity and conversations. The collected data may include, but is not limited to, recorded telephone conversations; location information of vehicles, digital devices, or persons at specific points in time; photographs of vehicles and subjects; and International Mobile Subscriber Identity. The data collected using third-party surveillance technology may be stored on a device or transmitted to a central-location data base, or Internet-connected computer using a cellular, radio, or satellite modem embedded in the unit. Data encryption may be a feature of the technology used by third parties, but the SCCDA has no authority to dictate the specific security features. Non-county entities independently contract with vendors providing surveillance technology and are not required to choose vendors that satisfy the data protection procedures outlined in Section 5 of this Surveillance Use Policy.

4. Data Access

The data collected by SCCDA employees using approved third-party surveillance technology 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 the third-party surveillance-technology data covered by this Policy shall be limited to 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.

5. Data Protection

See Sections 3 and 4 of this Policy. 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 SCCDA employees using third-party surveillance technology from unauthorized access, destruction, use, modification, or disclosure.

6. Data Retention

Data collected by SCCDA employee use of third-party surveillance technology, 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, which states 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.
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 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.

7. Public Access

Absent a court order, the public shall not have direct access to data collected by SCCDA employee use of third-party surveillance technology. 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 SCCDA employee use of third-party surveillance technology 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 SCCDA employees using third-party surveillance technology. 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. Sanctions for violation of this Surveillance Use Policy may range from counselling to termination, and in more serious breaches, may result in criminal prosecution.

Approved as to Form and Legality

1/5/19

Rob Coelho, Office of the County Counsel