Cellular Communications Interception Technology (CCIT) Usage and Privacy Policy

The Santa Clara County District Attorney's Office (SCCDA) investigates and prosecutes crime in Santa Clara County and supports victims of crime. The Office works tirelessly to hold offenders accountable and protect victims, and innovates to break the cycle of crime.

Authorized Purposes for Use of CCIT

The Santa Clara County District Attorney's Office (SCCDA) is an operator and end-user of cellular communications interception technology (CCIT), which is but one tool among many traditional law enforcement strategies and will only be employed in cases in which the technology is appropriate to achieve specific public safety goals. This technology will only be utilized when authorized by a search warrant or court order.

To support the mission of the SCCDA, authorized users with a need and right to know will intercept wire and electronic communications and communication information pursuant to, and in compliance with, a court order or search warrant under Penal Code section 629.50 *et seq* to investigate the following crimes:

- Murder, solicitation to commit murder, or the commission of a felony involving a destructive device, in violation of Penal Code sections 18710, 18715, 18720, 18725, 18730, 18740, 18745, 18750, or 18755;
- Any felony violation of Penal Code sections 11418 when relating to weapons of mass destruction, section 11418.5 when relating to threats to use weapons of mass destruction, or section 11419 when relating to restricted biological agents;
- Any felony criminal street gang offense or enhancement in violation of Penal Code section 186.22;
- The importation, possession for sale, transportation, manufacture, or sale of controlled substances in violation of Health and Safety Code sections 11351, 11351.5, 11352, 11370.6, 11378, 11378.5, 11379, 11379.5, or 11379.6 with respect to a substance containing heroin, cocaine, PCP, methamphetamine, or their precursors or analogs where the substance exceeds 10 gallons by liquid volume or 3 pounds of solid substance by weight;
- Any human trafficking offense in violation of Penal Code section 236.1; and
- An attempt or conspiracy to commit any of the above-mentioned crimes.

Authorized users with a need and right to know will intercept dialing, routing, addressing, or signaling information with CCIT pursuant to, and in compliance with, a court order or search warrant under Penal Code sections 638.52 and 638.63 for the following purposes:

- Recovery of stolen or embezzled property;
- Locating property or things used as the means of committing a felony;
- Locating property or things in the possession of a person with the intent to use them as a means of committing a public offense, or in the possession of another to whom he or she

may have delivered them for the purpose of concealing them or preventing them from being discovered;
- Locating evidence that tends to show a felony has been committed, or tends to show that a particular person has committed or is committing a felony;
- Locating evidence that tends to show that sexual exploitation of a child, in violation of Penal Code section 311.3, or possession of matter depicting sexual conduct of a person under 18 years of age, in violation of section 311.11, has occurred or is occurring;
- Locating a person who is unlawfully restrained or reasonably believed to be a witness in a criminal investigation or for whose arrest there is probable cause;
- Locating evidence that tends to show a violation of section 3700.5 of the Labor Code, or tends to show that a particular person has violated section 3700.5 of the Labor Code; and
- Locating evidence that does any of the following:
    - Tends to show that a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code, has been committed or is being committed;
    - Tends to show that a particular person has committed or is committing a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code; and
    - Will assist in locating an individual who has committed or is committing a felony, a misdemeanor violation of the Fish and Game Code, or a misdemeanor violation of the Public Resources Code.

Authorized Users of CCIT

The following individuals involved in the investigation and prosecution of crime are authorized to use CCIT ("authorized users"):

- District Attorney Investigators;
- Sworn peace officers and federal law enforcement officers working with SCCDA to investigate and prosecute crime and authorized to do so by court order pursuant to Penal Code section 629.54; and
- Designated civilian interpreters authorized by court order pursuant to Penal Code section 629.58.

All authorized users shall utilize CCIT only when authorized to do so by court order or search warrant, and their use of CCIT shall be limited by the parameters of the court order or search warrant.

Restrictions on Use of CCIT

All uses of CCIT will be done in a manner that is consistent with the United States and California Constitutions and federal and state law, including the Electronic Communications Privacy Act (ECPA) (California Penal Code section 1546 *et seq*), California's wiretap statutes (California Penal

Code section 629.50 *et seq*), 18 U.S. Code sections 2703, 3122, and 3123, and California Government Code section 53166.

Cellular communications interception technology is a restricted-use asset that is physically secured in a locked facility and electronically secured via password protection. The use of CCIT requires pre-approval of the District Attorney and judicial authorization via court order or search warrant.

Data received from CCIT may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution.

All SCCDA and authorized law enforcement and civilian monitor personnel utilizing CCIT are required to acknowledge that they have previously read and understood the SCCDA policy.

In no case shall data or information derived from the use of CCIT 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 CCIT. The training addresses appropriate handling and transmission procedures, as well as consequences of a security breach.

Only SCCDA staff and authorized law enforcement personnel and civilian monitors trained in the use of CCIT, including its privacy and civil liberties protections, shall be allowed to use CCIT. Training shall consist of:

- Legal authorities, requirements, developments, and issues involving the use of CCIT and data;
- Current SCCDA policy regarding appropriate use of CCIT;
- Evolution of CCIT, including new capabilities and associated risks;
- Technical, physical, administrative, and procedural measures to protect the security of CCIT 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 CCIT.

Authorized users shall be trained by the manufacturers of the CCIT and/or an authorized trainer within the SCCDA. Training shall be updated as technological, legal, and other changes that affect the use of CCIT systems occur.

Authorized users and SCCDA staff who access, maintain, disseminate, or audit CCIT data and information shall be familiar with this policy, the Electronic Communications Privacy Act (ECPA),

and California wire and electronic surveillance statutes (Penal Code sections 629.50 *et seq*). All SCCDA staff and associated law enforcement and civilian personnel who utilize CCIT will be certified by the California Office of the Attorney General in the interception of wire and electronic cellular telephone communications pursuant to Penal Code section 629.94 prior to using SCCDA CCIT.

CCIT Information Security

Access to communications and data derived from CCIT 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 CCIT from unauthorized access, destruction, use, modification, or disclosure.

CCIT Accuracy and Legal Compliance

Communications intercepted by CCIT shall be recorded on recording media in a manner that will protect the recording from editing or other alterations and ensure that the recording can be immediately verified as to authenticity and originality and that any alteration can be immediately detected. CCIT precludes interruption or monitoring of the interception by any unauthorized means. The CCIT manufacturer or its designated technician shall complete periodic assessments of the technology to ensure it is operating correctly and shall verify the technology is in proper working order prior to its use in an investigation. Authorized users shall periodically verify the accuracy of information intercepted through independent means during investigation and shall report any malfunctions of equipment.

CCIT Information Sharing Restrictions

The SCCDA only shares CCIT information with authorized law enforcement partners for public safety purposes and in compliance with Penal Code section 629.50 *et seq*. Additionally, pursuant to Penal Code section 1054 *et seq*, *Brady v. Maryland*, and Penal Code section 629.70, SCCDA provides CCIT information as criminal discovery to the appropriate defense or appellate attorney of record. SCCDA does not share CCIT information with commercial or other private entities or individuals.

CCIT Data Retention

In accordance with Penal Code sections 629.64 and 629.66, wire and electronic communications intercepted with CCIT will be kept for at least 10 years and shall not be destroyed except upon an order of the issuing or denying judge.

In accordance with the SCCDA Record Retention and Destruction Policy, CCIT data and communication information not governed by Penal Code sections 629.64 and 629.66 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 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.