Ventura County Sheriff's Office

SPECIAL SERVICES DIVISION

Standard Operating Procedures

SUBJECT: **CELLULAR COMMUNICATIONS INTERCEPTION TECHNOLOGY**

DATE	REVISION DATE:	PREPARED BY:	AUTHORIZED BY:
January 1, 2016	April 19, 2017	R. Thomas Captain	D. Kenney Commander

PURPOSE:

Establish usage and privacy guidelines for cellular communications interception technology.

DEPARTMENTAL IMPACT

Special Services - Major Crimes Bureau - Technical Services Unit

REFERENCES

California Government Code §53166

PROCEDURE

Background:
On January 1, 2016, Senate Bill 741 went into effect. SB 741 created California Government Code (CGC) section 53166. CGC 53166 requires law enforcement agencies that operate cellular communications interception technology (CCIT) to maintain reasonable security procedures and practices to protect information gathered through the use of CCIT from unauthorized access, destruction, use, modification, or disclosure. CGC section 53166 also requires agencies to implement a usage and privacy policy to ensure that collection, use, maintenance, sharing, and dissemination of information gathered through the use of CCIT complies with all applicable law and is consistent with individual privacy and civil liberties. The new law requires the usage and privacy policy to be available in writing to the public and to be posted conspicuously on the law enforcement agency's Internet Web site.

As with any law enforcement capability, the Ventura County Sheriff's Office must use CCIT in a manner that is consistent with the requirements and protections of the United

States and California Constitutions, as well as federal and state law, including the Electronic Communications Privacy Act (ECPA), California Penal Code Sections 1546 – 1546.4, 18 U.S.C. § 2703, 3122, 3123, which were enacted by the Legislature in Senate Bill 178 during the same legislative session as SB 741. The use of CCIT and any information collected through the use of CCIT must comply with the requirements of California Government Code 53166 and the ECPA.

ANALYSIS

In response to the creation of Government Code 53166, this policy has been updated to include several additions.

Definition:
CCIT (cellular communications interception technology) is defined as any device or technology that intercepts mobile telephone calling information, including international mobile subscriber identity catchers or other virtual based transceiver stations that masquerade as a cellular station and logs mobile telephone calling information.

AUTHORIZED PURPOSES:

1) CCIT provides valuable assistance in support of important public safety objectives. Whether deployed as part of a fugitive apprehension effort (including the use of "ESN" or "IMSI" registration capture), to assist in the investigation of felony crimes, to locate at-risk people or missing children, or to provide search and rescue support in natural disasters and emergencies, CCIT fulfills critical operational needs. For the purpose of this policy, the term fugitive includes individuals wanted for felony arrest warrants. All uses of CCIT will be in compliance with state and federal law. CCIT is but one tool among many traditional law enforcement strategies and will only be employed in cases in which the technology is best suited to achieve specific public safety goals. This technology will only be utilized when authorized by a search warrant that has been reviewed through the judicial process and is signed by a judicial officer (Penal Code Section 1546.1(b)(1)), (d)),(18 U.S.C. § 2703,3122,3123). All search warrants written for the authorized use of CCIT equipment maintained by the Technical Services Unit (TSU) must be reviewed and authorized by the Special Services Division Commander or his/her designee.

2) The Ventura County Sheriff's Office may use CCIT in the wake of a natural disaster or other emergency involving danger of death or serious bodily injury to any person, where the ability to locate a victim's cell phone can assist first responders in narrowing the area of a search, or locate victims and render aid in the shortest possible time frame (Penal Code Section 1546.1(c) (5)). In emergency circumstances involving a danger of death or serious bodily injury where the Sheriff's Office needs access to electronic information without delay, a search warrant shall be obtained within 72 hours of the use of CCIT (Penal Code Section 1546.1(c)(5) and (h)), (18 U.S.C. § 2703,3122,3123).

3) The Sheriff's Office may also use CCIT without a warrant if the Sheriff's Office, in good faith, believes the device to be lost, stolen, or abandoned, provided the Sheriff's Office shall only access electronic device information in order to attempt to identify, verify, or contact the owner or authorized possessor of the device.

AUTHORIZED EMPLOYEES:

A CCIT device may only be operated by TSU personnel who have received CCIT-specific training. TSU personnel will include sworn Deputy Sheriffs and Sheriff Service Technicians designated by the Major Crimes Captain. TSU personnel who operate a CCIT device shall be trained by the manufacturers of the CCIT device or an authorized trainer within the Sheriff's Office. Authorized TSU employees must attend refresher training as deemed necessary by the manufacturer. Sheriff's Office personnel, who access, maintain, disseminate, or audit CCIT device data shall ensure compliance with this policy and the ECPA, California Penal Code Sections 1546-1546.4. In addition, authorized TSU personnel will receive on-going training with respect to changing laws that impact the use of the CCIT device. For the purpose of this policy, authorized employees will only be assigned to the TSU.

SECURITY PROCEDURES:

CCIT is a restricted use asset. Physical safeguards include that when not in use, Ventura County Sheriff's Office's CCIT devices and technology are secured in a locked facility. Technical safeguards shall include that all CCIT access information is password protected. The password shall be unique to the CCIT and shall not be distributed to unauthorized users. Information gathered by CCIT shall also be password protected and only accessible by Sheriff's Office members trained by the manufacturer in the use of CCIT. Operational safeguards include that the use of any CCIT devices or technology shall require the pre-approval of the Special Services Division Commander or his/her designee and that each request that results in an approved use is supported by a search warrant or an applicable exemption under the ECPA. When making any application for a search warrant, Sheriff's Office members shall disclose appropriately and accurately the underlying purpose and investigative activities for which the order or authorization is sought and shall otherwise comply with the search warrant requirements of the ECPA, (18 U.S.C. § 2703, 3122, 3123), Penal Code Sections 1546.1and 1546.2, and the search warrant requirements of Part 2, Title 12, Chapter 3, Penal Code Sections 1523-1542.5.

TSU staff will maintain a CCIT usage log, which shall at minimum include: case number, type of investigation, the existence of a court order or detailed justification for the use of CCIT, the identity of the employee(s) operating CCIT, and the identity of the employee authorizing the use of CCIT.

The TSU Sergeant shall perform quarterly audits to assure the CCIT is performing as designed and staff is adhering to security and usage protocols. Audits shall be documented on the CCIT usage log.

CCIT usage logs shall be stored and maintained by TSU staff, and they may be destroyed after three years from the usage date.

PRIVACY AND CIVIL LIBERTIES:

The Ventura County Sheriff's Office is committed to ensuring that law enforcement practices concerning the use of CCIT are lawful, and appropriately respects the important privacy interests of individuals. CCIT may not be used for the sole purpose of monitoring individual activities protected by the First Amendment to the United States Constitution. All use of CCIT shall meet the requirements set forth in California Government Code 53166 and the ECPA. Any public records requests for information obtained by CCIT must be in accordance with California Public Records Act (CPRA), and Ventura County Sheriff's Office - General Order 810. Records of police investigations are generally exempt from public disclosure under Government Code Section 6254(f). Moreover, police records of information collected using CCIT will generally be considered official information acquired in confidence by authorized personnel which is privileged from disclosure under California Evidence Code Section 1040 and therefore exempt from public disclosure pursuant to Government Code Section 6254(k). Affidavits and applications in support of search warrants for information collected using CCIT are judicial records and are subject to disclosure by the Superior Court that issues the warrant, California Penal Code Section 1534(a). To the extent that electronic information accessed or obtained through the execution of a search warrant is recorded, the record may be considered to be a judicial record, Penal Code Section 1536. California Rules of Court, Rule 2.400(a) states that unless otherwise provided by court rules or ordered by the court, court records can only be inspected by the public in the office of the court. Judicial records are not subject to the California Public Records Act, Government Code Section 6252(f).

TRAINING AND ACCOUNTABILITY PROVISIONS:

Accountability is an essential element in maintaining the integrity of the use of CCIT by the Ventura County Sheriff's Office. Periodic review of this policy and training shall be the responsibility of the Special Services Division Commander or his/her designee with respect to the way the equipment is being used or the data is being collected (e.g., significant advances in technological capabilities, type of data collected, or the manner in which it is collected). Sheriff's Office members will be trained on this policy and comply with all orders concerning the use of this technology. Moreover, as the law in this area evolves, this policy will be amended to reflect the current state of the law. It is vital that all authorized users of CCIT familiarize themselves with the contents of this policy and the full content of the ECPA (PC 1546-1546.5) (18 U.S.C. § 2703, 3122, 3123), so that their administration of CCIT, and their court filings and representations are accurate and consistent with both the intent and scope of this policy. The Special Services Division Commander or his/her designee will ensure that members of the

Sheriff's Office who receive data from the use of a CCIT will comply with applicable federal and state discovery laws in criminal matters.

The monitoring of the use of CCIT devices or technology will be the responsibility of the Special Services Assistant Sheriff or his/her designee. Compliance checks with this usage and policy will be completed every fiscal quarter by the Special Services – Major Crimes Captain.

INFORMATION SHARING

The purpose of, process for, and restrictions on, the sharing of information to other law enforcement agencies:

1) The purpose of sharing information obtained by a CCIT device by the Ventura County Sheriff's Office to other law enforcement agencies is to provide a tool that many agencies do not have.
2) Process – Any law enforcement agency who has a written agreement with the Ventura County Sheriff's Office may request the use of the CCIT device. Any internal request within the Sheriff's Office or outside agency request, will be made through the TSU Sergeant. The TSU sergeant will review the request and ensure the request fall within the guidelines of this policy and applicable state and federal laws.
3) Restrictions - In the event an outside agency is provided with data obtained by a CCIT device, that agency will be required to sign a written agreement indicating the requesting agency will follow the guidelines of this policy.

The Ventura County Sheriff's Office often works closely with its Federal, State and Local law enforcement partners and provides technological and investigative assistance under a variety of circumstances. This policy applies to all instances in which the Ventura County Sheriff's Office uses CCIT in support of other Federal, State or Local law enforcement agencies. The Ventura County Sheriff's Office may share CCIT with other law enforcement agency partners that comply with this policy, all applicable state and federal laws, including the ECPA, the California Government Code, and the California Public Records Act, regarding the uses and restrictions from sharing information, including the purposes of, processes for, and limitations from sharing information.

A written agreement will be in place between the Ventura County Sheriff's Office and any other law enforcement agency before the sharing of any lawfully obtained data from CCIT.

INFORMATION RETENTION AND DISSEMINATION:

The Ventura County Sheriff's Office will operate CCIT in accordance with rules, policies, and laws that control the collection, retention, dissemination, and disposition of records that contain personal identifying information. As with data collected in the course of any investigation, these authorities apply to information collected through the use of CCIT.

The Ventura County Sheriff's Office will not collect, retain or disseminate any data except as authorized by this policy and by law. Consistent with applicable existing laws and requirements, including any duty to preserve and disclose exculpatory evidence, the Ventura County Sheriff's Office's use of CCIT shall include the following operational practices:

1) After the use of a CCIT under the authority of a search warrant to **locate** a cell phone, no data will be stored internally by the CCIT device. Only suspect or target data will be retained by the affiant of the search warrant. The affiant of the search warrant will comply with the suspect or target data under the guidelines of California ECPA.

2) When the equipment is used following a disaster, or in a search and rescue context, all data must be deleted as soon as the person or persons in need of assistance have been located and in any event no less than once every (10) days.

3) In the event a CCIT device is used under the authority of a search warrant to identify cell phones possessed by a suspect of a felony crime, the data obtained may be stored in the CCIT device for up to (30) days from the issuance of the search warrant. The process of using a CCIT device to identify unknown cell phones is commonly referred to as a Target Registration. After the 30 days, the data will be deleted from the CCIT device. Only suspect or target data will be retained by the affiant of the search warrant. All non-suspect data will be sealed by the court and will not be used for any purposes unless later determined by a court order to be pertinent. The affiant of the search warrant will comply with the suspect or target data under the guidelines of California ECPA.

4) The Ventura County Sheriff's Office shall implement an audit program to ensure that the data is deleted as described in sections 2 and 3 above. This audit shall take place not less than once every six (6) months. The audit program will be administered by the Special Services Division Commander or his/her designee.

5) In the event a criminal case is going to be or has been filed with a District Attorney's Office, State Attorney General's Office or United States Attorney General's Office, target or suspect data will be provided to these prosecutorial agencies while complying with applicable discovery laws and California ECPA. A written investigative report will be written by the affiant of the search warrant describing the data received by the CCIT device. A copy of this written report will be provided to the appropriate prosecutorial entity.

6) Any data or information obtained through the use of CCIT shall be considered Sensitive Controlled Information (SCI). Any records of SCI that are created shall only be accessed in conjunction with the need to know and right to know the data or information being sought, in accordance with the Ventura County Sheriff's Office policy regarding the release of SCI, General Order 810.

7) An updated copy of this entire policy will be available to the general public on the Ventura County Sheriff's Office – Public Website – VCSD.org.