

Cellular Site Simulator Usage and Privacy

609.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance and set guidelines and requirements pertaining to the use of cellular site simulator (CSS) technology.

609.2 POLICY

It is the policy of the Fontana Police Department to respect the privacy rights and civil liberties of individuals and to follow the Constitution and all applicable laws including Government Code section 53166.

609.3 BASIS FOR POLICY

Cell-site simulator technology significantly enhances the Department's efforts to achieve its public safety and law enforcement objectives. The CSS can be deployed in numerous ways. Whether as part of a fugitive apprehension effort, hostage negotiations, complex narcotics investigation, or to locate or rescue a kidnapped child, the simulator can fulfill critical operational needs. This policy provides guidance and establishes common principals designed to ensure that the Department deploys the CSS in an effective, appropriate and consistent way. The Department's various units that will utilize the CSS may issue additional specific guidance consistent with this policy.

609.4 AUTHORIZED USE

Cell-site simulator technology may be used to gather information leading to the identity or whereabouts of fugitives, suspects, victims or missing persons. Authorized department operators can use the simulator to help locate cellular devices whose unique identifiers are already known to law enforcement, or to determine the unique identifiers of an unknown device by collecting limited signaling information from the devices in the simulator user's vicinity

Cell-site simulators provide only the relative signal strength and general direction of a subject's cellular telephone. They do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Cell-site simulators used by the Department shall not be used to collect the contents of any communication or any data contained on the phone itself, such as emails, texts, contact lists, images or any other data from the phone. In addition, the CSS does not provide subscriber account information (for example, an account holder's name etc.).

The following are possible instances where CSS technology may be used:

- (a) Locate missing persons
- (b) Locate at-risk individuals

Cellular Site Simulator Usage and Privacy

- (c) Locate victims of mass casualty incidents/assistance in recovery efforts
- (d) Assist in investigations involving danger to the life or physical safety of an individual
- (e) Apprehend fugitives
- (f) Complex narcotic investigations

609.5 LEGAL AUTHORITY

Whenever possible, a search warrant shall be obtained prior to the use of the CSS. In the event the CSS is deployed under exigent circumstances without a warrant, by law, a search warrant must be obtained within 72 hours of its use. The CSS operator will be responsible for ensuring that the proper legal paperwork is obtained and maintained. The case agent requesting the CSS should normally be responsible for writing the warrant or a court order. The information obtained from the use of the CSS shall only be utilized and accessed by the CSS operator and involved case agent.

Regardless of the legal authority relied upon, at the time of making an application for the use of a CSS, the application supporting affidavit should describe in general terms the technique to be employed. The description should indicate that investigators plan to send signals to the cellular phone that will cause it, and non-target phones on the same provider network in close proximity, to emit unique identifiers, which will be obtained by the technology, and the investigators will use the information collected to determine information pertaining to the physical location of the target cellular device or to determine the currently unknown identifiers of the target device. The investigator will use the equipment to determine unique identifiers at multiple locations and /or multiple times at the same location. The application should indicate that also.

609.6 AUTHORIZED USERS AND TRAINING REQUIREMENTS

Personnel authorized to use or access information collected through the use of cell-site simulator technology shall be specifically trained in such technology and authorized by the Chief of Police or designee. Such personnel shall be limited to designated sergeants and officers unless otherwise authorized.

Training requirements for the above employees include completion of training by the manufacturer of the cell-site simulator or appropriate subject matter experts. Training updates are required annually.

609.7 DEPLOYMENT AND AGENCY MONITORING

Use of the CSS must be approved by a Lieutenant or a Special Operations or Investigations Unit Sergeant. The CSS operator will ensure the use of the equipment will be in support of a public safety operation or criminal investigation. The CSS shall not be utilized unless the proper legal process has been followed, including either obtaining a search warrant or submitting an exigent request form with a telephone/communications company.

Fontana Police Department

Fontana PD Policy Manual

Cellular Site Simulator Usage and Privacy

In all cases where the CSS is deployed, the operator will complete a CSS deployment form. The form must be signed by the operator and the approving supervisor who approved the use, and forwarded to the Special Operations Lieutenant for review.

The Fontana Police Department is committed to ensuring that the collection and retention of data is lawful and appropriately respects the privacy interests of individuals. Fontana Police 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 exculpatory evidence, the Department's use of the CSS shall include the following privacy practices:

- (a) When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is physically located and no less than once daily.
- (b) 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(s) in need of assistance has been located, and no less than once every ten days.
- (c) Prior to deploying the equipment for any mission, the CSS operator must verify that the equipment has been cleared of any previous operational data.
- (d) When a suspect is known to have been in two geographical different areas, any data collected in an effort to identify the cellular device shall be deleted upon completion of the mission, unless that data collected is deemed to have evidentiary value.

Data collected by the device, which is retained for the investigation, shall only be shared with those involved within the investigation or when ordered produced as part of a legal compliance process.

The Special Operations Lieutenant or his/her designee shall conduct audits to ensure that the data is being deleted in compliance in the above manner. These audits shall take place no less than once every six months. The audits will be documented and kept in the CSS file in the Special Operations Lieutenant's office.

609.8 DEPLOYMENT LOG

A CSS usage log shall be completed by the operator tracking every use of the CSS by the Department. The log shall contain:

- (a) Date(s)/time(s) of use
- (b) Suspected crime(s), if applicable
- (c) Location(s) used
- (d) Associated case numbers, if applicable
- (e) Phone number and /or device ID
- (f) The unit, or outside agency case agent and case number
- (g) Whether a phone was successfully located or identified