Special Order

Cellular Communications Interception Technology

This Special Order policy will govern the use of the Long Beach Police Department's ("LBPD") cell site simulator (CSS) and is written to comply with Government Code section 53166, effective January 1, 2016.

The use of a CSS device provides valuable assistance in support of public safety objectives. Whether deployed as part of a search and rescue mission in a natural disaster, a terrorist event, fugitive apprehension, or to locate at-risk people or missing children, the CSS device fulfills a critical operational need. The CSS device saves countless hours of surveillance and investigative effort by helping detectives quickly locate and arrest suspects wanted for criminal offenses.

This policy shall serve to ensure that the CSS technology is used in a manner consistent with the requirements and protections of the U.S. Constitution, including the Fourth Amendment, and applicable statutory authorities. Moreover, any information obtained from the use of a CSS device must be handled in a way that is consistent with all applicable laws, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data. As such, either a search warrant or exigent circumstances must exist prior to utilizing the CSS device.

In cases where the CSS device is deployed under exigent circumstances, by law, a search warrant must be obtained within three days of its use. The CSS operator will be responsible for ensuring that the proper legal paperwork is maintained.

The CSS computer, and any information obtained from it, shall only be utilized and accessed by authorized detectives in the Gang and Violent Crimes Division of the LBPD who have attended requisite training provided by the vendor.

Use of the CSS device must be approved by the Sergeant of the Career Criminal Apprehension Team (CCAT) or by his or her chain of command. Prior to approval, the CSS operator will ensure the use of the equipment will be in support of a public safety operation or criminal investigation and 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/telecommunications company. The CCAT sergeant is responsible for conducting periodic audits to ensure compliance with obtaining search warrants prior to using the CSS device, as well as auditing exigent circumstances to ensure search warrants are obtained within three days.

In all cases where the CSS is deployed, the authorized operator will complete a CSS deployment form. The form must be signed by the operator responsible for the operation and the CCAT Sergeant who approved the operation.

The form will be forwarded for review to the Lieutenant of the Crimes Against Persons

Section and the Commander of the Gang and Violent Crimes Division. After all review and signatures are obtained, the form will be returned to CCAT for retention in the CSS deployment file.

Any requests from another law enforcement agency to assist them with the use of the CSS device shall only be approved if it meets the criteria explained herein and LBPD policies and procedures are followed during its deployment. No deployment will take place until the proper legal paperwork (i.e., search warrant or exigent request) has been provided to the LBPD and has been reviewed to ensure it meets the legal requirements for use of the CSS device. If the request is approved, the CSS deployment form will be completed.

The CSS equipment will be secured and maintained in a locked LBPD facility when not in the field. Access to the equipment will only be allowed to authorized personnel within the CCAT chain of command or those approved by the Gang and Violent Crimes Division Commander, or his or her designee.

The LBPD is committed to ensuring that the collection and retention of data is lawful and appropriately respects the privacy interests of individuals. The LBPD 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 a CSS shall include the following privacy practices:

- 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.
- 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.
- Prior to deploying the equipment for any mission, the CSS operator must verify that the equipment has been cleared of any previous operational data.
- When a suspect is known to have been in two separate geographically different areas, any data collected in an effort to identify the cellular device shall be deleted upon completion of the mission, unless the 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 CCAT Sergeant shall conduct audits to ensure that the data is being deleted in compliance with the above manner. These audits shall take place no less than once every six months. The CCAT Sergeant will document these audits and submit them for review to the Lieutenant of the Crimes Against Persons Section. The audits will be

maintained in a file with the Crimes Against Persons Lieutenant and retained in compliance with the Department's business document retention policy.