FACT SHEET

Prepared by Detective II Mark Castillo
Major Crimes Division

Background:

On January 24, 2013, L.A. Weekly newsgroup published an article written by Jon Campbell, regarding the Los Angeles Police Department's (LAPD) use of "secretive cell phone spy devices." This article appeared to be in response to a recent Freedom of Information Act request from the First Amendment Coalition, requesting information regarding LAPD's cell phone tracking methods. This fact sheet has been prepared to address misinformation contained in the article and to provide clarification regarding the talking points that are portrayed in the article. The below "Issues" are quotes taken directly from the article, and are written in italics.

Issue 1: *A secretive cellphone spy device known as StingRay, intended to fight terrorism, was used in far more routine LAPD criminal investigations, 21 times in a four-month period during 2012, apparently with the courts' knowledge that the technology probes the lives of non-suspects who happen to be in the same neighborhood as suspected terrorists.*

Response: Any deployment of electronic monitoring equipment/techniques by the LAPD requires judicial review as a component of its implementation. Any electronic monitoring equipment utilized is limited in its scope and cannot disclose the personal information of a cellular telephone user without having undergone judicial review. Any deployment of electronic monitoring equipment/techniques must be within the Federal Statue as described in Title 18 2703(d), which requires that a Court Order be obtained for the disclosure of customer communications or records.

Issue 2: *As L.A. Weekly first reported in September, LAPD purchased StingRay technology sometime around 2006 with federal Department of Homeland Security funds. The original DHS grant documents said it was intended for "regional terrorism investigations." But the newly released LAPD records show something markedly different: StingRays are being deployed for burglary, drug and murder investigations.*

Response: Any current electronic monitoring equipment was purchased with non-Federal money. The current electronic monitoring equipment has not been intended for terrorism investigations alone, but was meant to be utilized in the apprehension of wanted suspects involved in a variety of crimes which pose a danger to the public at large. These crimes have included homicide, kidnapping, robbery, rape and narcotics investigations. In addition, electronic monitoring equipment has been utilized to locate individuals that are in distress or have medical conditions that pose an immediate danger to lives.

Issue 3: *Peter Scheer, executive director of the First Amendment Coalition, says the documents released by LAPD acknowledge "that they do have this technology, and that they're using*

it…But the documents are ambiguous about whether or not the procedure requires a warrant or other judicial permission."

Response: During the course of these cellular investigations they are subject to the scrutiny of judicial review and a signed court order as described in Title 18 2703(d). In the case of exigent circumstances (threat of death or great bodily injury), requiring an immediate response and deployment of electronic monitoring equipment, a court order signed by a judge is still due within 48 hours from the time exigency was determined.

Issue 4: *The portable StingRay device impersonates a cellphone tower, electronically fooling all nearby mobile phones, not just the suspect's phone, to send their signals into an LAPD computer. That signal reveals to police the location of phones in real time. But the technology sucks up the data of every cellphone in the area, and these innocent phone owners never know police are grabbing their information. Security researcher Chris Soghoian last year warned that StingRays can jeopardize privacy: "If the government shows up in your neighborhood, essentially every phone in the neighborhood is going to check in with the government…It's almost like Marco Polo, the government tower says 'Marco', and every cellphone in the area says 'Polo.'"*

Response: Any electronic monitoring equipment/techniques utilized by the LAPD can only gather data regarding the cellular phones in the area of a particular cell tower and from a particular carrier at any one time. This data only identifies the cellular phone by its carrier (i.e. Sprint, Metro PCS, Verizon) and gives no information regarding the subscriber's identity or their location. In order to identify a particular handset, it is necessary to have the cooperation of the cellular provider, which provides the necessary identifiers. This cooperation will only occur after being served with a signed court order. The cooperation of the cellular provider is governed by the Communications Assistance for Law Enforcement Act (1994), which mandates cellular providers to modify the design of their equipment, facilities and services to allow law enforcement to conduct electronic surveillance.

Issue 5: *Privacy advocates are troubled by StingRay's "self-service" aspects: Police can use the technology to get around the now-routine process of requesting location data from cellphone service providers. Carriers like Sprint and AT&T require that LAPD get a court order. StingRay could let police bypass the service providers entirely, and secretly.*

Response: Any electronic monitoring equipment/techniques utilized by the LAPD cannot be employed in the role of cell tracking without the cooperation of the cellular providers. For every single use of this technology a court order signed by a judge is necessary to maintain this cooperation. The LAPD operates within the parameters of U.S. Code Title 18 and the Communications Assistance for Law Enforcement Act. The cellular providers also employ the same standards to ensure that judicial review is in effect and will not disclose information to law enforcement without legal process.

Issue 6: *The records suggest that LAPD doesn't explicitly describe StingRay but instead seeks a judge's permission to use a "pen register/trap and trace," which is technology from landline days that functions like a caller ID, can't zero in on a person's real-time location like StingRay, and doesn't grab dozens or hundreds of innocent phone users in its web. Equating StingRay with a "pen register/trap and trace," Lye says, is like applying for a search warrant for someone's home and then searching the entire apartment complex. "The government has the duty of candor when it goes to the court," she says. "If in fact they got court orders 21 times, and these were the court orders they sought, they were in no way disclosing the technology they were using, and that is very troubling."*

Response: The use of the term "pen register/trap and trace" is used to describe the technology where by a cellular provider displays the location of a cell tower used by the cell phone that is the subject of court order. The term is related to older technology of landline services but is now used to describe the interaction between cellular towers and the cell phones that operate on them. With judicial review, law enforcement uses the cell tower information provided by the cellular provider to assist in locating the specific cell phone in question. The electronic monitoring equipment/techniques that are employed utilize only the data for the cell phone that is the subject of the court order. It cannot give a precise address of the cell phone handset and does not give any identifying information on its own. There is no interception of voice communications like a wire, although a court order is used in both instances. The laws operate differently with regards to a wire and the equipment which is the subject of this article, does not have the capability or authority to listen to conversations similar to that of a wire. The electronic monitoring equipment/techniques provide a refinement of the location of a specific cell phone handset based on the cell tower information provided by the cellular provider.

Should you have any questions, please contact Detective David Lott, Major Crimes Division, at (213) 216-5368.