

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,  
v.  
PURVIS LAMAR ELLIS, et al.,  
Defendants.

Case No. 13-CR-00818 PJH

**PRETRIAL ORDER NO. 3 DENYING  
MOTIONS TO SUPPRESS**

Doc. nos. 304, 307

United States District Court  
Northern District of California

On August 2, 2017, the court held a hearing on the motions of defendant Purvis Lamar Ellis to suppress evidence obtained from use of Stingrays on behalf of all defendants; to suppress evidence seized from Apartment 212 on behalf of all defendants; and to sever. The court DENIED Ellis’s motion to sever for the reasons stated on the record. Doc. no. 306. Having considered the relevant legal authority, the papers, argument of counsel, and the evidence in the record, the court DENIES the motions to suppress, doc. nos. 304, 307, for the reasons stated at the hearing and set forth below.

**I. Motion to Suppress Evidence Obtained from Use of Cell Site Simulators**

Ellis moves on behalf of all defendants to suppress any and all evidence obtained or derived from the use of cell site simulators (“CSS”), generally referred to as Stingrays. Doc. no. 304. As described in the Department of Justice Policy Guidance (“DOJ Policy”) cited by Ellis, a CSS functions by transmitting as a cell tower, such that cell phones in its proximity transmit signals to the CSS, which the cell phones identify as the most attractive cell tower in the area. Doc. no. 304 at 3-5 (citing *United States v. Patrick*, 842 F.3d 540, 542–43 (7th Cir. 2016) (quoting DOJ Policy, Sept. 3, 2015), *reh’g and reh’g en banc denied* (May 9, 2017)). “When used to locate a known cellular device, a cell-site

United States District Court  
Northern District of California

1 simulator initially receives the unique identifying number from multiple devices in the  
2 vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device  
3 for which it is looking, it will obtain the signaling information relating only to that particular  
4 phone.” *Id.* (internal marks omitted). See also doc. no. 321, Ex. G ¶ 6 and Ex. I ¶ 6.

5 As supported by the record, Ellis has shown that the Oakland Police Department  
6 (“OPD”) and the Federal Bureau of Investigation (“FBI”) each used a Stingray to locate  
7 Ellis’s cell phone starting in the early morning hours of January 22, 2013, following the  
8 shooting of an OPD officer the evening of January 21, 2013. Ellis contends that the use  
9 of these Stingrays amounted to a warrantless search requiring suppression of any  
10 evidence obtained or derived from the Stingrays, and/or an evidentiary hearing. Ellis  
11 further contends that the use of the Stingrays likely intercepted communications in  
12 violation of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

13 **A. Fourth Amendment Search**

14 **1. Legal Standard**

15 The Fourth Amendment provides in relevant part that “[t]he right of the people to  
16 be secure in their persons, houses, papers, and effects, against unreasonable searches  
17 and seizures, shall not be violated.” *United States v. Jones*, 565 U.S. 400, 404 (2012).  
18 The proponent of a motion to suppress has the burden of establishing that his own Fourth  
19 Amendment rights were violated by the challenged search or seizure. *Simmons v. United*  
20 *States*, 390 U.S. 377, 389-390 (1968).

21 The Supreme Court recognizes two tests to determine whether a “search” within  
22 the meaning of the Fourth Amendment occurred. *Jones*, 565 U.S. at 411. The first is the  
23 “classic” common-law trespass test, as applied by the Court in *Jones*. 565 U.S. at 404-  
24 05. Under that property-based approach, government actions amount to a search when  
25 “[they] physically occupy private property for the purpose of obtaining information” without  
26 consent. *Id.* The Court explained that before Justice Harlan’s concurrence in *Katz*  
27 articulated the “reasonable expectation of privacy” standard, “for most of our history the  
28 Fourth Amendment was understood to embody a particular concern for government

United States District Court  
Northern District of California

1 trespass upon the areas (“persons, houses, papers, and effects”) it enumerates.” *Jones*,  
2 565 U.S. at 406. The Court in *Jones* held that attachment of a Global Positioning System  
3 (GPS) tracking device to a vehicle, and the subsequent use of that device to monitor the  
4 vehicle’s movements on public streets, was a search within the meaning of the Fourth  
5 Amendment, reasoning that “[t]he Government physically occupied private property for  
6 the purpose of obtaining information. We have no doubt that such a physical intrusion  
7 would have been considered a ‘search’ within the meaning of the Fourth Amendment  
8 when it was adopted.” *Id.* at 404-05 (citation omitted).

9 Second, under the reasonable expectation of privacy test, the Fourth Amendment  
10 protects against an unreasonable search of an area in which (1) a person exhibits actual,  
11 subjective expectation of privacy, and (2) the expectation is one that society is prepared  
12 to recognize as reasonable. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J.,  
13 concurring). Under *Katz*, the capacity to claim Fourth Amendment protection does not  
14 strictly depend on a property right in the invaded place, but whether the person asserting  
15 the claim has a legitimate expectation of privacy. *Rakas v. Illinois*, 439 U.S. 128, 143  
16 (1978) (citing *Katz*, 389 U.S. at 353).

17 **2. Use of Stingray Constitutes a Search**

18 Ellis asserts several grounds for determining that the use of the Stingray to locate  
19 his cell phone in real time amounted to a Fourth Amendment search requiring issuance of  
20 a warrant: that the Stingray intruded into the constitutionally protected area of a private  
21 residence and that the Stingray violated Ellis’s privacy interests both in the use and  
22 location of his cell phone and in his public movements.

23 In his reply, Ellis raises the argument that the government is bound by its  
24 concession in other cases that the use of a Stingray amounts to a search. Doc. no. 324  
25 at 2-3. However, the court finds that these concessions were limited for the purposes of  
26 each particular case, and do not amount to a binding admission by the government. See  
27 *Patrick*, 842 F.3d at 544, 545 (where the government conceded that use of a cell site  
28 simulator is a search for purposes of that litigation, the court noted that questions about

United States District Court  
Northern District of California

1 whether use of a simulator amounts to a search “have yet to be addressed by any United  
2 States court of appeals,” reserving the issue).

3 **a. Standing**

4 As a threshold matter, the government contends that only Ellis has standing to  
5 challenge the use of a Stingray to locate his cell phone, and that no other defendant has  
6 standing to bring a motion to suppress. To the extent that Ellis challenges the potential  
7 collection of signals from phones used by non-parties, the government correctly points  
8 out that Ellis lacks standing to invoke the privacy rights of anyone else whose cell phone  
9 may have been located by the Stingrays. In light of the record showing that two  
10 Stingrays were used to locate Ellis’s cell phone, and no other defendant’s cell phone,  
11 Ellis alone has standing to bring the instant motion to suppress evidence obtained  
12 through use of Stingrays. See *Rakas*, 439 U.S. at 133-34 (“Fourth Amendment rights are  
13 personal rights which, like some other constitutional rights, may not be vicariously  
14 asserted.”) (citation and marks omitted).

15 **b. Intrusion on Private Residence**

16 Starting with the *Jones* trespassory approach, Ellis argues that the government’s  
17 use of the Stingrays to monitor and track his phone was a search under the Fourth  
18 Amendment because the Stingrays emitted signals that penetrated the walls of private  
19 dwellings that were not open to visual surveillance. Doc. no. 304 at 15 (citing *United*  
20 *States v. Karo*, 468 U.S. 705, 714 (1984) and *Kyllo v. United States*, 533 U.S. 27, 29  
21 (2001)). In *Karo*, the Court held that the warrantless “monitoring of a beeper in a private  
22 residence, a location not open to visual surveillance, violates the Fourth Amendment  
23 rights of those who have a justifiable interest in the privacy of the residence.” In *Kyllo*,  
24 the Court held that use of a thermal-imaging device aimed at a private home from a  
25 public street to detect relative amounts of heat within the home constitutes a “search”  
26 within the meaning of the Fourth Amendment, reasoning that “obtaining by sense-  
27 enhancing technology any information regarding the interior of the home that could not  
28 otherwise have been obtained without physical intrusion into a constitutionally protected

1 area' [ ] constitutes a search—at least where (as here) the technology in question is not  
2 in general public use.” 533 U.S. at 34 (quoting *Silverman v. United States*, 365 U.S. 505,  
3 512 (1961)). Ellis argues that because a Stingray emits signals that penetrate the walls  
4 of constitutionally protected spaces, it amounts to trespass and constitutes a search  
5 under *Silverman*, 365 U.S. at 511-12 (holding that attaching a spike mike to a heating  
6 duct of a home was a search, reasoning that technical trespass is not necessary for  
7 Fourth Amendment violation but “actual intrusion into a constitutionally protected area” is  
8 sufficient) and *Jones*, 565 U.S. at 410 (holding that warrantless installation of GPS device  
9 to vehicle encroached on a protected area in violation of Fourth Amendment).

10 The government responds that Ellis lacks standing to assert any protected interest  
11 in the apartment where he was located because he was in someone else’s home when  
12 the Stingray located his cell phone, not his own residence which was known to be  
13 Apartment 212. Opp. at 6. If Ellis had been in someone else’s private residence at the  
14 time his cell phone was located by the Stingray, he could not strictly assert a violation of  
15 any property-based or privacy-related interest in that residence. See *Kyllo*, 533 U.S. at  
16 34-35 and *Karo*, 468 U.S. at 714.

17 Ellis argues that there is no evidence in the record to support the government’s  
18 position that Ellis was not in his own home when his cell phone location was detected at  
19 a specific apartment. The record indicates that Ellis and other occupants of Apartment  
20 112 were escorted out of the building at around 10:52 am, but it is not clear from the  
21 record where Ellis was located when the Stingray tracked his cell phone location. The  
22 evidence in the record only suggests that the Stingray, in conjunction with “a cell site  
23 simulator augmentation device,” located Ellis’s cell phone at a particular location that is  
24 not identified in the declarations. See doc. no. 321, Ex. I (declaration of unnamed FBI  
25 Special Agent whose identifying information was redacted to protect his identity, see doc.  
26 no. 244 (8/8/16 transcript) at 15-16; previously submitted in this case as doc. no. 225-1).

27 The record is therefore insufficient to determine whether Ellis had any protectable  
28 interest in the residence where his cell phone was located. It is unnecessary to decide

United States District Court  
Northern District of California

1 this issue of Ellis’s standing to claim Fourth Amendment protection for the private  
2 residence, however, because Ellis does have standing to challenge the use of the  
3 Stingray to locate his cell phone based on a reasonable expectation of privacy in one’s  
4 real-time cell phone location, as discussed below.

5 **c. Reasonable Expectation of Privacy in Real-Time Location**  
6 **of Cell Phones**

7 Under the *Katz* test, Ellis has demonstrated that the use of the Stingray devices  
8 amounted to a search in violation of a reasonable expectation of privacy in the real-time  
9 location of his cell phone.

10 The Ninth Circuit has not decided the question presented here whether use of cell  
11 site simulators to locate cell phones in real time amounts to a search, nor the issue  
12 whether there is a reasonable expectation of privacy in one’s cell phone location. In  
13 *Patrick*, the first circuit court opinion to address the use of Stingrays, the Seventh Circuit  
14 noted that the issue remains unsettled as to whether the use of cell site simulators  
15 amounts to a search, by analogy to GPS locators which are treated as searches when  
16 police enter private property to install them under *Jones*, and which may impinge on  
17 expectations of privacy when used for long-term monitoring. *Patrick*, 842 F.3d at 543-44  
18 (citing *Jones*, 565 U.S. at 413-31 (concurring opinions of Sotomayor and Alito, JJ.)). The  
19 court in *Patrick* also discussed the competing view that the use of cell site simulators is  
20 more like the use of a pen register, which is not a search because it reveals the making  
21 of a call and the number called but not the call’s communicative content, or the use of a  
22 beeper, which is not a search because it reveals a suspect’s location but nothing else.  
23 *Id.* (citing *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Knotts*, 460 U.S.  
24 276 (1983)). *Patrick* did not, however, decide this question because the government  
25 “conceded for the purpose of this litigation that use of a cell-site simulator is a search.”  
26 *Id.* at 544.

27 In the absence of controlling authority, Ellis suggests that *Riley v. California*, 134  
28 S. Ct. 2473, 2489-90 (2014), should be extended to recognize a protected privacy

United States District Court  
Northern District of California

1 interest in the use and location of cell phones. The Court in *Riley* held that a warrant is  
2 generally required to search the information on a cell phone, recognizing the privacy  
3 interests in the kinds of data stored on or accessed through modern cell phones, but did  
4 not go so far as to hold that the Fourth Amendment protects the use or location of a cell  
5 phone in real time.

6 The storage capacity of cell phones has several  
7 interrelated consequences for privacy. First, a cell phone  
8 collects in one place many distinct types of information—an  
9 address, a note, a prescription, a bank statement, a video—  
10 that reveal much more in combination than any isolated  
11 record. Second, a cell phone’s capacity allows even just one  
12 type of information to convey far more than previously  
13 possible. The sum of an individual’s private life can be  
14 reconstructed through a thousand photographs labeled with  
15 dates, locations, and descriptions; the same cannot be said of  
16 a photograph or two of loved ones tucked into a wallet. Third,  
17 the data on a phone can date back to the purchase of the  
18 phone, or even earlier. A person might carry in his pocket a  
19 slip of paper reminding him to call Mr. Jones; he would not  
20 carry a record of all his communications with Mr. Jones for the  
21 past several months, as would routinely be kept on a phone.

22 Finally, there is an element of pervasiveness that  
23 characterizes cell phones but not physical records. . . .  
24 According to one poll, nearly three-quarters of smart phone  
25 users report being within five feet of their phones most of the  
26 time, with 12% admitting that they even use their phones in  
27 the shower. . . . [I]t is no exaggeration to say that many of the  
28 more than 90% of American adults who own a cell phone  
keep on their person a digital record of nearly every aspect of  
their lives—from the mundane to the intimate. . . .

Although the data stored on a cell phone is  
distinguished from physical records by quantity alone, certain  
types of data are also qualitatively different. . . . Data on a cell  
phone can also reveal where a person has been. . . .

*Riley*, 134 S. Ct. at 2489–90 (footnote and citations omitted). Though this discussion is  
instructive, *Riley* did not recognize a protected privacy interest in one’s cell phone use or  
location.

On a related issue, several judges in this district have recognized a right to privacy  
in historical cell site location information (“CSLI”) that is collected by cellular service  
providers. CSLI is generated by the radio signals emanated by a cell phone to the  
closest cell tower in the cellular service network, as described more fully by Judge Koh in

1 *In re Application for Telephone Information Needed for a Criminal Investigation*, 119 F.  
2 Supp. 3d 1011, 1013-15 (N.D. Cal. 2015), No. 15-xr-90304 HRL (LHK), doc. no. 30,  
3 *appeal dismissed* (Feb. 5, 2016). “The resulting CSLI includes the precise location of the  
4 cell tower and cell site serving the subject cell phone during each voice call, text  
5 message or data connection,” and may be generated even without the user’s interaction  
6 with the cell phone. *Id.* at 1014 (citations omitted).

7 Judge Illston addressed the privacy interests in such information in *United States*  
8 *v. Cooper*, 2015 WL 881578 (N.D. Cal., Mar. 2, 2015), No. 13-cr-693 SI, doc. no. 117.  
9 There, the defendant moved to suppress evidence obtained from collecting historical and  
10 prospective, or real-time, cell site location information without a warrant. Judge Illston  
11 recognized that cell phone users have a reasonable expectation of privacy in their  
12 physical location as conveyed by historical CSLI that is protected by the Fourth  
13 Amendment. *Id.* at \*6-11 (citing *United States v. Davis*, 754 F.3d 1205, 1215 (11th Cir.),  
14 *vacated*, 573 Fed. Appx. 925 (11th Cir. 2014), *and reheard en banc in part*, 785 F.3d 498  
15 (11th Cir. 2015)). Judge Illston did not reach the Fourth Amendment issue with respect  
16 to prospective CSLI, but held, as further discussed below at pp. 16-17, that by application  
17 of the Communications Assistance of Law Enforcement Act (“CALEA”), 47 U.S.C.  
18 § 1002(a)(2), the pen register statute did not authorize access to call-identifying  
19 information from telecommunications carriers that may disclose the subscriber’s physical  
20 location, and that a showing of probable cause was required to obtain prospective cell  
21 site data. *Id.* at \*3-6. Although the government had not obtained a warrant, the court  
22 denied the motions to suppress upon finding that the agents relied in good faith on the  
23 magistrate judge’s order authorizing a pen register. *Id.* at \*11-12.

24 Judge Koh also held that cell phone users have a reasonable expectation of  
25 privacy in historical CSLI, requiring a warrant to obtain such information absent case-  
26 specific exceptions. *In re Appl. for Tel. Info.*, 119 F. Supp. 3d at 1025-26. There, the  
27 government submitted an application to Magistrate Judge Lloyd for an order authorizing it  
28 to obtain both historical and prospective CSLI for target cell phones pursuant to the



United States District Court  
Northern District of California

1 Stored Communications Act (“SCA”), 18 U.S.C. § 2703(d), which sets forth a “specific  
2 and articulable facts” standard that requires a lesser showing than probable cause.  
3 Following *Cooper*, Magistrate Judge Lloyd denied the application and required the  
4 government to obtain a search warrant to obtain cell site information, whether historical or  
5 prospective. No. 15-xr-90304 HRL (LHK), doc. no. 2.

6 The government appealed Magistrate Judge Lloyd’s denial with respect to the  
7 application for historical CSLI. In affirming that decision, Judge Koh articulated several  
8 Fourth Amendment principles based on Supreme Court precedent:

9 (1) an individual’s expectation of privacy is at its pinnacle  
10 when government surveillance intrudes on the home; (2) long-  
11 term electronic surveillance by the government implicates an  
12 individual’s expectation of privacy; and (3) location data  
generated by cell phones, which are ubiquitous in this day and  
age, can reveal a wealth of private information about an  
individual.

13 *In re Appl. for Tel. Info.*, 119 F. Supp. 3d at 1022. Applying those principles to the  
14 government’s application for historical CSLI, Judge Koh determined that the information  
15 sought by the government was arguably more invasive of an individual’s expectation of  
16 privacy than the GPS device attached to the defendant’s car in *Jones*, noting that when  
17 the government uses CSLI data to obtain information about one’s location and  
18 movements, (1) “an individual will invariably enter constitutionally protected areas, such  
19 as private residences” and (2) the government would “get more information, more data  
20 points, on the cell phone via historical CSLI” compared to GPS tracking of a car, because  
21 cell phones typically accompany the user wherever she goes. *Id.* at 1023 (internal marks  
22 omitted). Applying the *Katz* test, Judge Koh considered evidence demonstrating that  
23 individuals have a subjective expectation of privacy in the historical CSLI associated with  
24 their cell phones, and determined that society is prepared to recognize that expectation  
25 as objectively reasonable, citing state court decisions recognizing a reasonable  
26 expectation of privacy in CSLI. *Id.* at 1024-26. Upon determining that the third party  
27 doctrine did not defeat that reasonable expectation of privacy, and that no exception to  
28

1 the warrant requirement was applicable, Judge Koh held that the Fourth Amendment  
2 requires the government to secure a warrant to obtain historical CSLI. *Id.* at 1040.

3 In *United States v. Williams, et al.*, 2016 WL 492934 (N.D. Cal. Feb. 9, 2016), No.  
4 13-cr-764 WHO, doc. no. 874, Judge Orrick followed *In re Application for Telephone*  
5 *Information and Cooper* to recognize a reasonable expectation of privacy in one's  
6 historical CSLI, requiring probable cause to obtain the historical CSLI from the four  
7 moving defendants' cell phones. Having determined that the government submitted  
8 several applications pursuant to the SCA under the lower "specific and articulable facts"  
9 standard rather than the probable cause standard, Judge Orrick held that the good faith  
10 reliance exception applied and denied the motions to suppress.<sup>1</sup> 2016 WL 492934 at \*2.

11 On the specific issue presented here whether using a Stingray to locate a cell  
12 phone amounts to a search, the district court for the Southern District of New York held  
13 that the DEA's use of a CSS to locate a defendant's apartment "was an unreasonable  
14 search because the 'pings' from [the defendant's] cell phone to the nearest cell site were  
15 not readily available 'to anyone who wanted to look' without the use of a cell-site  
16 simulator." *United States v. Lambis*, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016) (quoting  
17 *Knotts*, 460 U.S. at 281), *appeal withdrawn* (Mar. 13, 2017). The court in *Lambis* rejected  
18 the government's contention that there was no reasonable expectation of privacy under  
19 the third party doctrine, reasoning that the location information detected by a cell-site  
20 simulator is "neither initiated by the user nor sent to a third party," unlike pen register  
21 information that is conveyed to a telephone company or cellular provider. 197 F. Supp.

22  
23  
24  
25  
26  
27  
28

---

<sup>1</sup> By separate order, doc. no. 873, Judge Orrick granted another defendant's motion to suppress historical CSLI obtained under a warrant, which the court determined was not supported by probable cause, having recognized a reasonable expectation of privacy in one's historical CSLI. *United States v. Williams*, 161 F. Supp. 3d 846, 850-57 (N.D. Cal.) (order granting A. Gilton's motion to suppress cell phone data) (citing *In re Appl. for Tel. Info. and Cooper*), *appeal docketed*, No. 16-10109 (9th Cir. March 11, 2016). The Ninth Circuit recently withdrew submission of the appeal from the suppression order pending the Supreme Court's decision in *Carpenter v. United States*, No. 16-402, which presents the question whether warrantless search and seizure of historical cell phone records revealing the location and movements of cell phones is permitted under the Fourth Amendment. *Williams*, CR 13-cr-764 WHO, doc. no. 1194.

1 3d at 614-15. *See also State v. Andrews*, 227 Md. App. 350, 393 (2016) (holding that  
2 people have a reasonable expectation of privacy in real-time cell phone location  
3 information, and requiring a search warrant to use a CSS); *State v. Tate*, 357 Wis. 2d 172  
4 (2014) (assuming, without deciding, that use of a Stingray amounted to a Fourth  
5 Amendment search requiring a warrant, and holding that the pen register order was  
6 sufficiently particularized and based on probable cause).

7 The government relies on recent circuit court decisions that tracking cell site  
8 location information from phone companies is not a search because there is no  
9 reasonable expectation of privacy in information shared with cellular service providers  
10 under the third party doctrine. *United States v. Graham*, 824 F.3d 421, 435-38 (4<sup>th</sup> Cir.  
11 2016) (en banc), *pets. for cert. filed sub nom Graham v. United States*, No. 16-6308  
12 (Sept. 26, 2016) and *Jordan v. United States*, No. 16-6694 (Oct. 27, 2016); *United States*  
13 *v. Carpenter*, 819 F.3d 880, 888 (6<sup>th</sup> Cir. 2016), *cert. granted sub nom Carpenter v.*  
14 *United States*, No. 16-402 (June 5, 2017). Distinguishing these cases, the court in  
15 *Lambis* reasoned that unlike CSLI obtained by the wireless carriers, CSS technology has  
16 “an additional layer of involuntariness” that renders the third party doctrine inapplicable:

17 Unlike CSLI, the “pings” picked up by the cell-site simulator  
18 are not transmitted in the normal course of the phone’s  
19 operation. Rather, “cell site simulators actively locate phones  
20 by forcing them to repeatedly transmit their unique identifying  
electronic serial numbers, and then calculating the signal  
strength until the target phone is pinpointed.”

21 *Lambis*, 197 F. Supp. 3d at 615 (quoting *Andrews*, 227 Md. App. at 359 n.4). The court  
22 in *Lambis* also determined that unlike pen register information or CSLI, “a cell-site  
23 simulator does not involve a third party.” *Id.* at 616. “With the cell-site simulator, the  
24 Government cuts out the middleman and obtains the information directly.” *Id.* *See also*  
25 *Patrick*, 842 F.3d at 543 (noting that by using CSS technology, “law-enforcement officials  
26 get the same sort of information that a phone company could provide using its own  
27 facilities, and they get it in real time rather than waiting for the phone company to turn  
28

1 over data”). For the reasons articulated in *Lambis*, the circuit court decisions applying the  
2 third party doctrine to historical CSLI are inapposite.

3 The court adopts Judge Koh’s reasoning in *In re Application for Telephone*  
4 *Information*, 119 F. Supp. 3d at 1026, to hold that cell phone users have an expectation  
5 of privacy in their cell phone location in real time and that society is prepared to recognize  
6 that expectation as reasonable. While Judge Koh limited her analysis to the privacy  
7 interest in historical CSLI, the court determines that cell phone users have an even  
8 stronger privacy interest in real time location information associated with their cell  
9 phones, which act as a close proxy to one’s actual physical location because most cell  
10 phone users keep their phones on their person or within reach, as the Supreme Court  
11 recognized in *Riley*. In light of the persuasive authority of *Lambis*, and the reasoning of  
12 my learned colleagues on this court recognizing a privacy interest in historical cell site  
13 location information, the court holds that Ellis had a reasonable expectation of privacy in  
14 his real-time cell phone location, and that use of the Stingray devices to locate his cell  
15 phone amounted to a search requiring a warrant, absent an exception to the warrant  
16 requirement.

17 **d. Privacy Interest in One’s Public Movements**

18 Ellis further argues that because a Stingray can track an individual’s location by  
19 locating his cell phone with an accuracy of about two meters, its use infringed upon his  
20 reasonable expectation of privacy in one’s public movements, as considered by Justice  
21 Sotomayor in her concurring opinion in *Jones*: “GPS monitoring generates a precise,  
22 comprehensive record of a person’s public movements that reflects a wealth of detail  
23 about her familial, political, professional, religious, and sexual associations. . . . I would  
24 take these attributes of GPS monitoring into account when considering the existence of a  
25 reasonable societal expectation of privacy in the sum of one’s public movements.” Doc.  
26 no. 304 at 16 (citing *Jones*, 565 U.S. at 415-16 (Sotomayor, J., concurring)). The Court  
27 in *Jones* did not reach the question whether the Fourth Amendment protects a privacy  
28 interest in one’s public movements, and even Justice Sotomayor did not attempt to

1 resolve these “difficult questions” because “the Government’s physical intrusion on  
2 Jones’ Jeep supplies a narrower basis for decision.” *Id.* at 418. Accordingly, Ellis fails to  
3 establish that a reasonable expectation of privacy in one’s public movements that is  
4 protected under the Fourth Amendment has been recognized by any court.

5 **B. Pen Register Procedures**

6 The government argues that even if use of the Stingray devices amounted to a  
7 search, the search was reasonable because it was conducted pursuant to the emergency  
8 provisions of the pen register statute, in combination with provisions of the Stored  
9 Communications Act. The government further argues that a warrant was not required to  
10 conduct the search pursuant to the exception for exigent circumstances, and that the  
11 exceptions to the exclusionary rule for good faith reliance and/or inevitable discovery are  
12 also applicable.

13 The pen register statute and the SCA set forth different standards to authorize  
14 different methods of electronic surveillance. The provisions for authorizing a pen register  
15 and/or a trap and trace device under Title III of the Electronic Communications Privacy  
16 Act of 1986 (“ECPA”), codified as amended at 18 U.S.C. §§ 3121-3127 (referred to  
17 throughout as the “pen register statute”), require a government attorney merely to “certify”  
18 the relevance of the information likely to be obtained, without requiring a factual basis for  
19 the certification. 18 U.S.C. §§ 3122 and 3123 (requiring the court to enter “an ex parte  
20 order authorizing the installation and use of a pen register or trap and trace device  
21 anywhere within the United States, if the court finds that the attorney for the Government  
22 has certified to the court that the information likely to be obtained by such installation and  
23 use is relevant to an ongoing criminal investigation”). The SCA, enacted under Title II of  
24 the ECPA, as amended, provides that the government may require a provider of  
25 electronic communication service or remote computing service to disclose a subscriber’s  
26 records, without the contents of communications, by obtaining either (A) a warrant, or (B)  
27 a court order upon a showing of “specific and articulable facts showing . . . reasonable  
28 grounds to believe that . . . the records or other information sought, are relevant and

1 material to an ongoing criminal investigation.” 18 U.S.C. §§ 2703(c)(1) and (d). The  
2 “specific and articulable facts” standard under the SCA requires a higher showing than  
3 the certification required by the pen register statute, but does not require probable cause.

4 Under the emergency provisions of the pen register statute, a law enforcement  
5 officer who reasonably determines that an emergency situation exists may have a pen  
6 register or trap and trace device installed without a prior court order only if an order  
7 approving the installation or use is issued within forty-eight hours after the installation has  
8 occurred, or begins to occur. 18 U.S.C. § 3125. The provision for “Emergency Pen  
9 Register And Trap And Trace Device Installation” narrowly defines a covered  
10 “emergency” to involve specific circumstances, two of which the government asserts  
11 authorized the use of the emergency provisions here: (A) immediate danger of death or  
12 serious bodily injury to any person; and (B) conspiratorial activities characteristic of  
13 organized crime. 18 U.S.C. §§ 3125(a)(1)(A) and (B). The officers’ sworn statements,  
14 including affidavits filed under seal in this case, establish that the OPD had reason to  
15 believe that there was an emergency where (A) the immediate safety of officers and/or  
16 public citizens was at risk and (B) the emergency involved the conspiratorial activities of  
17 organized crime, based on information that Ellis was a known member of a gang who  
18 was involved in an attempted murder at a bus stop on January 20, who was near the  
19 shooting of a police officer earlier that evening on January 21, and who was believed to  
20 be in possession of guns.

21 It is undisputed that the OPD and FBI did not seek issuance of a search warrant to  
22 operate the Stingray devices, but only obtained an order authorizing pen register and/or  
23 trap and trace devices (the “pen register order”). Here, the state court judge issued an  
24 order pursuant to both the SCA and the pen register statute (“18 United States Code  
25 Section 2703(c)(d), 3122, 3123”) requiring the service providers to provide the FBI and  
26 the OPD with pen registers “to register numbers dialed or pulsed[,] to record the date and  
27 time[,] to record the length of time[,] and to receive cell site and/or location sites,” as well  
28 as trap and trace devices, for the target phone number which the application

1 demonstrated was used by Ellis. Doc. no. 321, Ex. F. The court order also required the  
2 wireless carriers to provide, “on an ongoing and/or real-time basis, the location of cell  
3 site/sector (physical address) at call origination (for outbound calls), call termination (for  
4 incoming calls), and, during the progress of a call, the direction and strength of a signal”  
5 for the target phone. The government does not contend that the order authorizing the  
6 use of pen register and/or trap and trace devices here was supported by a finding of  
7 probable cause. The pen register order does not make a probable cause finding, but  
8 only a finding of “specific and articulable facts establishing reasonable grounds to believe  
9 the listed records are relevant and material to an ongoing criminal investigation” pursuant  
10 to the SCA, 18 U.S.C. §§ 2703(c)(1)(B) and (d). Doc. no. 321, Ex. F.

11 Ellis contends that the pen register order was not sufficient to authorize the use of  
12 the Stingray devices, which required a warrant. As an initial matter, Ellis challenges the  
13 government’s factual assertion that the Stingrays were configured as pen registers and/or  
14 trap and trace devices, doc. no. 321 at 9 and Exs. G-J, given that Stingrays also have the  
15 capability of intercepting the content of communications, not just information about  
16 numbers dialed in or dialed out. Doc. no. 324 at 3. See 18 U.S.C. § 3127(3) and (4)  
17 (defining pen register as a device which “records or decodes dialing, routing, addressing,  
18 or signaling information” transmitted by the target phone on outgoing calls, and a trap and  
19 trace as a device which captures information from incoming calls made to the target  
20 phone, but not contents of any communication). Although Ellis seeks supporting  
21 evidence about how the specific Stingray devices were configured and the capabilities of  
22 each device, the sworn affidavits of the OPD and FBI agents are sufficient to establish  
23 that the Stingrays used here were configured as pen registers and/or trap and trace  
24 devices and were not capable of capturing any content. Doc. no. 321 at 9 and Exs. G-J.  
25 There is no evidence in the record suggesting that the Stingrays captured the content of  
26 any communications, and an evidentiary hearing to determine the mechanical details  
27 about the Stingray devices is not warranted.

28

1 Ellis further argues that even if the government had obtained a search warrant  
2 authorizing the use of the Stingrays, the warrant would be invalid for lack of particularity  
3 because a cell site simulator is capable of collecting information from anyone's phone  
4 that was within range. Doc. no. 304 at 19. He suggests that the FBI and OPD used the  
5 Stingrays to monitor potentially hundreds of individuals' phone calls. *Id.* at 22. This is a  
6 purely speculative argument given the sworn affidavits of the Stingray operators stating  
7 that the devices were configured to look for the phone number that belonged to Ellis.  
8 Doc. no. 321, Exs. G ¶ 8 (OPD officer) and I ¶ 10 (FBI agent). There is no evidence to  
9 suggest that Stingrays were set up to sweep all cell phones in the area, and such a  
10 configuration would be inconsistent with the purpose for using the Stingrays, which was  
11 to find Ellis by locating his cell phone.

12 The government contends that since the Stingray devices used in this case were  
13 configured in compliance with the pen register statute, then the provisions of the pen  
14 register statute, including the "emergency" provisions, govern their operation. Doc. no.  
15 321 at 9 (citing 18 U.S.C. § 3125). The government does not address the key issue in  
16 dispute, namely, whether the provisions of the pen register statute and the SCA provide  
17 the appropriate standard for using a CSS to locate a cell phone in real-time. The court  
18 follows Judge Illston's determination in *Cooper*, 2015 WL 881578, that the provisions of  
19 the pen register statute and the SCA do not authorize the use of a CSS to disclose real-  
20 time information about a cell phone user's physical location, and that such location  
21 monitoring must be authorized by a showing of probable cause.

22 In *Cooper*, the government collected both historical and prospective CSLI from  
23 Metro PCS pursuant to orders authorizing pen register, trap and trace, and cell site data,  
24 without the use of Stingrays or similar devices, and the defendant challenged the failure  
25 to show probable cause to obtain cell site data. With respect to obtaining prospective  
26 CSLI, the government argued in *Cooper* that it was not required to show probable cause  
27 but only needed to satisfy the provisions of the pen register statute, 18 U.S.C. § 3123,  
28 and the SCA, 18 U.S.C. § 2703(d).



1 With respect to real time CSLI, Judge Illston held that under the CALEA, which  
2 amended the ECPA, the government is prohibited from relying solely on the provisions of  
3 the pen register statute to obtain cell site data that discloses the physical location of the  
4 subscriber. *Cooper*, 2015 WL 881578 at \*3 (citing 47 U.S.C. § 1002(a)(2)(B) (“with  
5 regard to information acquired solely pursuant to the authority for pen registers and trap  
6 and trace devices [ ], such call-identifying information shall not include any information  
7 that may disclose the physical location of the subscriber)). Judge Illston noted that the  
8 CALEA did not explicitly establish a standard for obtaining cell site data, and applied the  
9 “default” probable cause standard of Rule 41 of the Federal Rules of Criminal Procedure.  
10 *Id.* (citations omitted). See Fed. R. Crim. P. 41(d)(1) (“After receiving an affidavit or other  
11 information, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of  
12 record--must issue the warrant if there is probable cause to search for and seize a person  
13 or property or to install and use a tracking device.”). Judge Illston rejected the  
14 government’s hybrid theory that combining the SCA with the pen register statute to obtain  
15 prospective cell site data would comply with the CALEA, reasoning that Congress  
16 intended that the SCA “was to be used as a means to obtain data which has **already**  
17 **been stored** at the time the government seeks to obtain it,” as opposed to real-time data.  
18 *Cooper*, 2015 WL 881578 at \*4-5 (emphasis added).

19 Here, the government has provided declarations stating that the OPD and FBI  
20 configured the Stingray devices to locate the target cell phone, not broadly tracking all  
21 cell phone signals in the apartment building, making the Stingray use here similar to use  
22 of a beeper that was tracked inside a home, as in *Karo*, 468 U.S. at 715 (“the monitoring  
23 indicated that the beeper was inside the house, a fact that could not have been visually  
24 verified”). Given the undisputed fact that the Stingray devices were configured to locate  
25 Ellis’s cell phone, the court adopts Judge Illston’s reasoning in *Cooper* to hold that by  
26 application of 47 U.S.C. § 1002(a)(2), the pen register statute in combination with the  
27 SCA does not authorize obtaining cell phone location information through pen register or  
28 trap and trace devices, and that a warrant supported by a showing of probable cause is

1 required to use a Stingray to locate a cell phone. The court further holds that the  
2 “specific and articulable facts” standard under the SCA does not govern the use of a  
3 Stingray on the separate ground that the SCA authorizes the disclosure of  
4 communications or records kept by third party service providers, not direct surveillance of  
5 cell phone location by the government.

6 The government raises a cursory argument that the search of Ellis’s cell phone  
7 location information was a valid probation search, contending that the more intrusive  
8 search of the contents of his cell phone was valid under the four-way search condition of  
9 his probation. Doc. no. 321 at 16 (citing 10/29/15 Order, hereby designated “Pretrial  
10 Order No. 2,” at 19). The government cites no authority for this proposition, given that  
11 the privacy interest in one’s cell phone location, which could be a proxy for one’s  
12 personal location, is more akin to the privacy interests against GPS tracking or GPS  
13 monitoring, which was not a condition of Ellis’s probation.

14 Accordingly, the warrantless searches were unreasonable, unless the exigent  
15 circumstances exception to the warrant requirement applies. If the court finds that no  
16 exception to the warrant requirement applies, the government seeks an exception from  
17 the exclusionary rule for good faith reliance or inevitable discovery.

18 **C. Exception to Warrant Requirement for Exigent Circumstances**

19 The government argues that if a warrant was required to use a Stingray to locate a  
20 cell phone, the warrantless searches here were reasonable due to exigent circumstances  
21 which relieved law enforcement of the warrant requirement. Doc. no. 321 at 10 (citing  
22 *Kentucky v. King*, 563 U.S. 452, 460 (2011) and *Murdock v. Stout*, 54 F.3d 1437, 1441  
23 (9<sup>th</sup> Cir. 1995), *abrogated on other grounds by United States v. Ramirez*, 523 U.S. 65, 69-  
24 70 (1998)). The government identifies several factors known to law enforcement to  
25 demonstrate exigent circumstances at the time the OPD and FBI deployed the Stingrays:

- 26 i. Ellis was identified by an eyewitness as the get-away driver in an  
27 attempted murder on January 20, 2013;
- 28 ii. The same eyewitness identified the license plate number of the car  
Ellis was driving, and that car was located in the rear lot of the

apartment building where Ellis lived;

- iii. The next day, an Oakland police officer investigating the get-away car was attacked, beaten, and shot while Ellis stood in the driveway of the apartments;
- iv. Ellis was in the driveway when the assault occurred;
- v. The guns stolen from the officer were in Ellis's room;
- vi. In the days immediately preceding the shooting, Ellis was in possession of a large number of firearms;
- vii. Ellis was a known member of a gang with a violent history; and
- viii. Ellis lived at the 1759 Seminary Apartment complex, but officers did not know his location.

Doc. no. 321 at 8. Having reviewed the affidavits in the record, including the unredacted search warrant affidavits and pen register application filed ex parte under seal, the court determines that these circumstances were known to OPD officers by the early morning of January 22, 2013, when the first Stingray was deployed. See doc. no. 321, Ex. M (under seal). Ellis disputes the government's factual assertions (iii) and (iv) suggesting that he was involved in the assault and shooting of the OPD officer. Doc. no. 324 at 2. Officer Saunders' redacted pen register application indicates, however, that B.O.T., known to be Ellis, was "in the driveway when the shooting happened." Doc. no. 304, Ex. I.

Under the exigency exception to the warrant requirement, officers may make a warrantless search if: (1) they have probable cause to believe that the item or place to be searched contains evidence of a crime, and (2) they are facing exigent circumstances that require immediate police action. *United States v. Camou*, 773 F.3d 932, 940 (9th Cir. 2014). Exigent circumstances are defined as "those circumstances that would cause a reasonable person to believe that entry [or search] ... was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *Id.* (quoting *United States v. McConney*, 728 F.2d 1195, 1199 (9th Cir. 1984) (en banc), *overruled on other grounds by Estate of Merchant v. Comm'r*, 947 F.2d 1390, 1392–93 (9th Cir. 1991)). "To be reasonable, a search under this exception

1 must be limited in scope so that it is ‘strictly circumscribed by the exigencies which justify  
2 its initiation.’” *Id.* (quoting *Mincey v. Arizona*, 437 U.S. 385, 393 (1978)).

3 Ellis disputes that any exigencies justified use of the Stingrays without a warrant  
4 sometime after 2:11 a.m., where earlier that evening, by 8:45 p.m., Ellis and other  
5 suspects had already been determined to be in the apartment building which had been  
6 surrounded by the SWAT team “to contain any suspects.” Doc. no. 324, Ex. C. Ellis also  
7 points out that the officers had time to apply for and obtain three separate search  
8 warrants late at night and into the morning, particularly the warrant to search Apartments  
9 108, 110 and 112, which Judge Horner issued at 1:05 am, indicating that the situation did  
10 not prevent the OPD and FBI from seeking court authorization to use the Stingrays. Doc.  
11 no. 324 at 7; doc. no. 321, Ex. B (search warrant).

12 Because the OPD and FBI proceeded on the premise that the Stingrays were  
13 subject to the emergency provisions of the pen register statute, rather than a warrant  
14 requirement, the government contends that the officers followed the statutory procedures  
15 by securing an order authorizing use of the Stingray devices within 48 hours of using the  
16 device. Doc. no. 321 at 9-10 (citing 18 U.S.C. § 3125). The order was issued on January  
17 22, 2013, the same day the Stingrays were used, although the exact time the order was  
18 issued is not known.

19 The government argues that exigent circumstances excused the requirement to  
20 obtain a warrant to locate Ellis’s cell phone, but Ellis responds that he was not known to  
21 have assaulted or directly threatened violence against the victim in either of the  
22 shootings. The record demonstrates, however, that Ellis was a known suspect involved  
23 as a getaway driver in the January 20 shooting and was near the January 21 shooting in  
24 the driveway. Though Ellis was not known to be the shooter, he was believed to be a  
25 suspect in possession of firearms. The need to prevent escape by a suspect presented  
26 exigent circumstances here. *McConney*, 728 F.2d at 1199. Although Ellis was not  
27 involved in an armed standoff situation, the timeline of events and the facts presented in  
28 the unredacted pen register application demonstrate that law enforcement officers on the

1 scene believed that any unnecessary delay in finding Ellis would endanger their lives or  
 2 the safety of others and/or that speed was essential to prevent his escape. *See Fisher v.*  
 3 *City of San Jose*, 558 F.3d 1069, 1075 (9th Cir. 2009) (en banc) (where exigent  
 4 circumstances justified seizure of the suspect who was seen pointing a rifle at police  
 5 officers, loading his rifles, and arranging them strategically throughout his apartment to  
 6 repel any entry by the police, police were not required to obtain an arrest warrant to take  
 7 the suspect into full physical custody over twelve hours later).

8 The declarations and documents in support of the government's opposition, doc.  
 9 no. 321, indicate the following sequence of events on the night of January 21 to January  
 10 22, 2013, as cited below.

11	9:00 pm	At about 9:00 pm, the Stingray operator for the OPD arrived at the scene, and helped deploy the SWAT robots soon after arriving. Ex. G ¶ 10.
12		
13	10:41 pm	Police held a perimeter on the apartment building at 1759 Seminary, and continued to search nearby houses, roofs, yards and a creek. 8/17/15 Order at 9.
14		
15	11:15 pm	OPD prepared an Exigent Circumstance Request to MetroPCS asking for call detail records, cell sites and pen register information for Ellis's cell phone number. Ex. A.
16		
17	11:55 pm	Officers end the yard search and focus on 1759 Seminary. 8/17/15 Order at 9.
18		
19	1:05 am	Judge Horner signed the warrant authorizing the search of Apartments 108, 110, and 212. Ex. B.
20	1:47 am	OPD starts making announcements for "everyone to stay away from windows," and preparing to send bean bags into Apartment 212. Doc. no. 304, Ex. M (CAD reports).
21		
22	2:11 am	OPD Officer Saunders faxed a Pen Worksheet for Ellis's number to Metro PCS, asking to "start pen register if phone is active and being used," implying that the pen register had not yet been provided. Ex. C. Sometime after that request was faxed, OPD obtained the pen register information and deployed the Stingray. Ex. G ¶¶ 11, 12 (indicating the OPD Stingray operator did not begin operating the Stingray until after OPD obtained the pen register information from the telephone provider, and began operating the Stingray sometime after midnight in the early hours).
23		
24		
25		
26		
27	3:41 am	OPD searched Apartment 212, finding both handguns taken from Officer K. plus a third pistol, and keys to the white Dodge Avenger
28		

1 getaway car from the January 20 daytime shooting. 8/17/15 Order at 10.

2 7:00 am At approximately 7:00 am, the FBI Stingray operator was notified that  
3 OPD requested assistance from the FBI in the use of its cell site simulator. Ex. I ¶ 8.

4 7:30 am The FBI sent MetroPCS an Exigent Circumstances Request for pen register information on Ellis's phone. Ex. D; Ex. I ¶ 9.

5 9:00 am The FBI Stingray operator arrived at the scene. Ex. I ¶ 10.

6 10:00 am OPD powered off its Stingray and purged the data, and the FBI  
7 began operating its Stingray. Ex. G ¶ 13, 15; Ex. I ¶ 10. The FBI  
8 Stingray was operated for about one hour before Ellis's phone was located. Ex. I ¶ 10.

9 10:52 am Apartment 112 was cleared, and Ellis and the other occupants were  
10 escorted out. Ex. L (radio purge excerpt)

11 Ellis suggests that OPD had sufficient time to obtain a warrant to deploy the Stingrays as  
12 demonstrated by the issuance of the search warrant for Apartments 108, 110 and 212 in  
13 the early hours of January 22. To explain why a warrant or pen register order was not  
14 obtained before deploying the Stingrays, the government has demonstrated that OPD  
15 proceeded under the emergency pen register procedures and that OPD otherwise would  
16 have needed to wait until normal business hours to submit a pen register order to  
17 MetroPCS. Doc. no. 321, Ex. K. Indeed, it is worth noting that the factual basis for  
18 demonstrating probable cause for issuance of the warrant authorizing the search of Ellis's  
19 apartment would have likely been found to support probable cause for the OPD to use  
20 the Stingray device to locate Ellis by locating his cell phone, if a separate warrant had  
21 been sought, based on the showing of a fair probability that evidence of a crime would be  
22 found. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). See doc. no. 307, Ex. E (search  
23 warrant affidavit sworn at 1:05 a.m. on 1/22/2013).

24 Ellis also suggests that there was no exigency requiring a warrantless search to  
25 prevent flight and to prevent harm to the officers and others because OPD knew that Ellis  
26 was somewhere inside the apartment building, rather than outside where police had  
27 conducted a search of nearby houses and yards. However, OPD obtained a warrant to  
28 search Ellis's residence, Apartment 212, and he was not there, leaving the entire building

1 to remain under siege all night as OPD continued to look for Ellis. Under these  
2 circumstances, the use of the Stingray by OPD to locate Ellis's cell phone was justified by  
3 exigent circumstances, based on risk of flight and the belief that Ellis was in possession  
4 of firearms. The FBI's use of the second Stingray device was a continuation of the  
5 OPD's initial search for Ellis's cell phone location. *See Fisher*, 558 F.3d at 1077-78  
6 ("officers were not required to periodically reassess whether the exigency persisted  
7 throughout the standoff because the standoff was 'no more than an actual continuation'  
8 of the actual seizure" and the exigent circumstances did not materially change) (citing  
9 *Michigan v. Tyler*, 436 U.S. 499, 511 (1978) (warrantless entry into burning building to  
10 extinguish fire and conduct search to determine its cause was justified by exigency, and  
11 warrantless post-fire search four hours later, despite the absence of exigent  
12 circumstances, was upheld as a continuation of the initial search); *United States v.*  
13 *Echegoyen*, 799 F.2d 1271, 1280 (9th Cir. 1986) (where exigent circumstances justified  
14 initial warrantless entry, subsequent entry by narcotics officers to inspect the premises for  
15 a possible fire hazard was merely a continuation of the initial lawful entry because both  
16 were done to alleviate the exigent circumstances)). *Cf. Michigan v. Clifford*, 464 U.S.  
17 287, 296 (1984) (post-fire search for evidence of arson "was not a continuation of an  
18 earlier search" where the homeowners made a reasonable effort to secure their fire-  
19 damaged home after the blaze was extinguished and the fire and police units left the  
20 scene about six hours earlier, distinguishing *Tyler*).

21 Accordingly, the court determines that a warrant was not required to deploy the  
22 Stingrays to locate Ellis's cell phone under the exigent circumstances that existed the  
23 morning of January 22, 2013. Ellis's motion to suppress evidence obtained from use of  
24 the Stingrays is therefore DENIED.

25 Notwithstanding this determination, the court proceeds to consider the exceptions  
26 to the exclusionary rule for good faith reliance and/or inevitable discovery asserted by the  
27 government as separate grounds for denying the motion to suppress.  
28

1           **D.       Exceptions to Exclusionary Rule**

2                   **1.       Good Faith Reliance**

3           The government argues that even if a warrant had been required to authorize the  
4 use of the Stingrays, the OPD officers and FBI agents reasonably relied in good faith on  
5 the pen register order, issued under the emergency procedures of the pen register  
6 statute, 18 U.S.C. § 3125, to use the Stingrays to locate Ellis’s cell phone.

7           The “good faith” exception to the exclusionary rule established by *United States v.*  
8 *Leon*, 468 U.S. 897 (1984), is satisfied if an officer acts “in objectively reasonable  
9 reliance” on a defective warrant. *See United States v. Underwood*, 725 F.3d 1076, 1084  
10 (9th Cir. 2013). “To determine whether the officer acted in objectively reasonable  
11 reliance, ‘all of the circumstances - including whether the warrant application had  
12 previously been rejected by a different magistrate - may be considered.’” *Id.* (citing *Leon*,  
13 468 U.S. at 922 n. 23; *Messerschmidt v. Millender*, 565 U.S. 535, 132 S. Ct. 1235, 1249-  
14 50 (2012)). The burden of demonstrating good faith rests with the government. *Id.*

15           The Court in *Leon* identified four situations that per se fail to satisfy the good faith  
16 exception: (1) where the affiant recklessly or knowingly placed false information in the  
17 affidavit that misled the issuing judge; (2) where the judge “wholly abandon[s] his [or her]  
18 judicial role”; (3) where the affidavit is “so lacking in indicia of probable cause as to render  
19 official belief in its existence entirely unreasonable” (in other words, a “bare bones”  
20 affidavit); and (4) where the warrant is “so facially deficient - i.e., in failing to particularize  
21 the place to be searched or the things to be seized - that the executing officers cannot  
22 reasonably presume it to be valid.” *Underwood*, 725 F.3d at 1085 (citing *Leon*, 468 U.S.  
23 at 922-23) (internal quotation marks omitted). “In these situations, ‘the officer will have  
24 no reasonable grounds for believing that the warrant was properly issued.’” *Id.* (quoting  
25 *Leon*, 468 U.S. at 922–23).

26           Ellis argues that any good faith reliance argument is foreclosed by the fact that  
27 Officer Saunders’s application failed to disclose to the issuing judge that the OPD and  
28 FBI planned to use the Stingray devices, rather than more traditional pen register and



1 trap and trace methods. Ellis points out that the pen register application does not, on its  
2 face, seek authorization to use a Stingray. Doc. no. 324 at 4-5. Under Ninth Circuit  
3 authority, however, the particular means of executing a warrant need not be specifically  
4 authorized, though it is subject to judicial review for reasonableness if challenged. *United*  
5 *States v. Chen*, 979 F.2d 714, 720 (9th Cir. 1992) (following *Dalia v. United States*, 441  
6 U.S. 238, 258-59 (1979) (“It would extend the Warrant Clause to the extreme to require  
7 that, whenever it is reasonably likely that Fourth Amendment rights may be affected in  
8 more than one way, the court must set forth precisely the procedures to be followed by  
9 the executing officers.”)). In *Dalia*, the Court held that the Fourth Amendment requires  
10 that search warrants must be issued by neutral, disinterested magistrates; that those  
11 seeking the warrant must demonstrate to the magistrate their probable cause to believe  
12 that the evidence sought will aid in a particular apprehension or conviction for a particular  
13 offense; and that warrants must particularly describe the things to be seized, as well as  
14 the place to be searched, but do not require “a specification of the precise manner in  
15 which they are to be executed.” *Dalia*, 441 U.S. at 255, 257 (citations and internal marks  
16 omitted). See *Patrick*, 842 F.3d at 544 (“neither constitutional text nor precedent  
17 suggests that ‘search warrants also must include a specification of the precise manner in  
18 which they are to be executed’”) (citing *Richards v. Wisconsin*, 520 U.S. 385 (1997) and  
19 *Dalia*, 441 U.S. at 256). In light of this authority, it was reasonable for Officer Saunders  
20 not to disclose the particular manner of execution in his application for a pen register  
21 order authorizing location information for Ellis’s cell phone, including cell site/sector  
22 location and “direction and strength of a signal” for his telephone number.

23 Ellis also challenges the pen register order on the ground that the order  
24 authorizing use of the devices for a period of 30 days from the date of the order could not  
25 have authorized the use of any device before the order was signed on January 22, 2013,  
26 but the government has explained that the statutory provisions for emergency pen  
27 register applications permit such post hoc authorization. 18 U.S.C. § 3125. Ellis further  
28 challenges the pen register order because the government has failed to produce the

1 original, but the lack of an original does not warrant suppression in light of other evidence  
2 in the record demonstrating that the pen register order was issued by Judge Horner.

3 Here, there are no indicia of bad faith where the Stingray operators have attested  
4 that the OPD and FBI configured the Stingrays as pen registers, without capturing any  
5 content of communications, and sought authorization under the pen register statute in  
6 combination with the SCA. The government points out that under then-existing FBI  
7 policy, a warrant was not required before using a cell site simulator. See doc. no. 304  
8 Ex. B (FBI Electronic Surveillance Manual at 41). The excerpt of a manual cited by Ellis  
9 further instructed that cell site simulators were covered by the definition of a pen register  
10 in 18 U.S.C. § 3127(3) as amended by the USA Patriot Act of 2001, Pub.L. 107–56,  
11 October 26, 2001, 115 Stat. 272. Doc. no. 304, Ex. O (USABook). That DOJ policy has  
12 since been amended, effective September 3, 2015, to require a warrant to operate a  
13 CSS. See *Lambis*, 197 F. Supp. 3d at 611.

14 At the time the CSS technology was used in this case, there was no controlling  
15 authority as to whether its use constituted a search requiring issuance of a warrant. In  
16 this district, Judge Illston’s unpublished decision in *Cooper*, 2015 WL 881578, requiring a  
17 showing of probable cause to obtain prospective cell site location information, was not  
18 issued until two years after the Stingrays were used in this case in January 2013.

19 On the other hand, there is out-of-district authority indicating that prior to 2013, the  
20 government applied for tracking warrants within this district, supported by a showing of  
21 probable cause, to use mobile tracking devices that acted like cell site simulators. In  
22 *Rigmaiden*, the government obtained a tracking warrant in this district issued in 2008 by  
23 then-Magistrate Judge Seeborg to use a mobile tracking device which functioned as a  
24 cell site simulator to locate the defendant’s aircard. *United States v. Rigmaiden*  
25 (*“Rigmaiden I”*), 844 F. Supp. 2d 982, 995 (D. Ariz. 2012) (“The mobile tracking device  
26 mimicked a Verizon Wireless cell tower and sent signals to, and received signals from,  
27 the aircard.”). The government conceded there, for purposes of the defendant’s requests  
28 for discovery related to his suppression motions, that the aircard tracking operation was a

1 Fourth Amendment search and seizure and that the government would rely on the Rule  
2 41 tracking warrant, application, and affidavit to authorize the use of the tracking device  
3 to communicate directly with the defendant's aircard and determine its location. *Id.* at  
4 996 (citing *In re Application of the US for an Order Authorizing the Use and Monitoring of*  
5 *a Mobile Tracking Device*, No. 08-xr-90330-RS (N.D. Cal.)). After conducting an ex parte  
6 hearing, and in light of the government's factual admissions and concessions, the  
7 Arizona district court denied the defendant's motions for disclosures and additional  
8 discovery. *See id.* at 1005 ("The Court concludes that Defendant has ample information  
9 with which to construct his Fourth Amendment arguments."). The court subsequently  
10 denied Rigmaiden's motion to suppress evidence with respect to the FBI's use of the  
11 mobile tracking device after determining that the tracking warrant was supported by  
12 probable cause. *United States v. Rigmaiden ("Rigmaiden II")*, 2013 WL 1932800 (D.  
13 Ariz. May 8, 2013). The court in *Rigmaiden II* initially determined that the defendant did  
14 not have a reasonable expectation of privacy in the aircard that was obtained through  
15 fraud. 2013 WL 1932800 at \*6-9. The Arizona district court did not, however, reach the  
16 issue whether use of a CSS required a warrant even if there was a protected privacy  
17 interest because the government conceded that use of a CSS-type mobile tracking  
18 device to track the aircard was a Fourth Amendment search and relied on a warrant,  
19 which the court found was supported by probable cause and sufficient particularity.

20 Prior to 2013, the few out-of-district courts presented with the question whether  
21 law enforcement was required to obtain a warrant or a pen register/trap and trace order  
22 to operate a cell site simulator, or similar device, issued differing opinions. *Compare In re*  
23 *Application of the U.S. for an Order Authorizing Use of a Cellular Telephone Digital*  
24 *Analyzer ("In re Appl. Digital Analyzer")*, 885 F. Supp. 197, 202 (C.D. Cal. 1995) (holding  
25 that no court order is required for law enforcement agents to use a digital analyzer to  
26 detect only the electronic serial number and phone number of the subject cellular  
27 telephone and the numbers being called, but, to the extent an order could be fashioned,  
28 requiring certain provisions analogous to an order authorizing a pen register and trap and

1 trace device pursuant to 18 U.S.C. § 3123(b)) *with In re Application of the U.S. for an*  
2 *Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device*, 890 F.  
3 Supp. 2d 747, 748 (S.D. Tex. 2012) (denying application for order authorizing the  
4 installation and use of a pen register and trap and trace device to operate “stingray” in the  
5 absence of authority that pen register statute, rather than warrant requirement, applies to  
6 stingray equipment) (citing *In re Appl. Digital Analyzer*).

7 In determining whether to apply the exclusionary rule in the absence of settled  
8 authority applicable to the use of new investigative technology, the court considers the  
9 Supreme Court’s observation that “under *Leon*’s good faith exception, we have ‘never  
10 applied’ the exclusionary rule to suppress evidence obtained as a result of nonculpable,  
11 innocent police conduct.” *Davis v. United States*, 564 U.S. 229, 240 (2011) (citing  
12 *Herring v. United States*, 555 U.S. 135, 144 (2009)).

13 When the police exhibit “deliberate,” “reckless,” or “grossly  
14 negligent” disregard for Fourth Amendment rights, the  
15 deterrent value of exclusion is strong and tends to outweigh  
16 the resulting costs. [*Herring*, 555 U.S. at 144.] But when the  
17 police act with an objectively “reasonable good-faith belief”  
18 that their conduct is lawful, *Leon*, [468 U.S.] at 909, or when  
19 their conduct involves only simple, “isolated” negligence,  
20 *Herring, supra*, at 137, the “deterrence rationale loses much  
21 of its force,” and exclusion cannot “pay its way.” See *Leon*,  
22 *supra*, at 919, 908, n. 6 [internal citation omitted].

23 *Id.* at 238. Here, the law enforcement officers took steps to obtain court authorization  
24 under the pen register procedures that they believed were applicable to use of the  
25 Stingrays for tracking the location of Ellis’s cell phone. Officer Saunders’s application did  
26 not mislead the issuing judge about the purpose of the pen register order, which included  
27 locating Ellis’s cell phone with information about “cell site and/or location sites” and “on  
28 an ongoing and/or real-time basis, the location of cell site/sector (physical address)” for  
outbound and incoming calls and “the direction and strength of a signal” during a call in  
progress. The application articulated specific facts and circumstances giving rise to the  
need to locate Ellis and his coconspirators. The pen register order did not amount to a

1 mere “rubber stamp” or otherwise indicate that the judge wholly abandoned his judicial  
2 role in approving the pen register application.

3 Under the totality of the circumstances, where the state court judge had reviewed  
4 a detailed affidavit which he found demonstrated probable cause to issue a search  
5 warrant earlier that morning, at 1:05 a.m., the OPD and FBI Stingray operators  
6 reasonably relied on the emergency pen register procedures to deploy the Stingray  
7 devices. In particular, the FBI relied in objectively good faith on then-current DOJ policy  
8 and practice construing the pen register statute to cover the use of cell site simulators. In  
9 *Illinois v. Krull*, 480 U.S. 340, 349 (1987), the Supreme Court recognized that the *Leon*  
10 exception applies if officers obtain evidence in objectively reasonable reliance on a  
11 statute that is subsequently declared unconstitutional, reasoning that “[t]here is no basis  
12 for applying the exclusionary rule to exclude evidence obtained when a law enforcement  
13 officer acts in objectively reasonable reliance upon a statute, regardless of whether the  
14 statute may be characterized as ‘substantive’ or ‘procedural.’” *Id.* at 356 n.12. In  
15 weighing whether suppression would have significant deterrent effect, the court in *Krull*  
16 determined as follows:

17 There is nothing to indicate that applying the exclusionary rule  
18 to evidence seized pursuant to the statute prior to the  
19 declaration of its invalidity will act as a significant, additional  
20 deterrent. Moreover, to the extent that application of the  
21 exclusionary rule could provide some incremental deterrent,  
22 that possible benefit must be weighed against the “substantial  
23 social costs exacted by the exclusionary rule.” [*Leon*, 468  
24 U.S. at 907.] When we indulge in such weighing, we are  
25 convinced that applying the exclusionary rule in this context is  
26 unjustified.

27 *Krull*, 480 U.S. at 353.

28 Because the FBI proceeded here under a mistaken understanding of the statute,  
rather than a statute that has been found unconstitutional, *Krull* does not squarely apply.  
However, the *Krull* analysis is instructive to determine whether applying the exclusionary  
rule would have significant deterrent effect to warrant suppression of evidence. Law  
enforcement’s view that the use of the Stingrays was authorized under the provisions of

1 the pen register statute, an unsettled question that has yet to be decided by any appellate  
2 authority, is distinguishable from a mistaken understanding of the law supporting a belief  
3 that a suspect has broken the law. *Cf. United States v. Lopez-Soto*, 205 F.3d 1101,  
4 1106–07 (9th Cir. 2000) (officer lacked reasonable suspicion to stop defendant based on  
5 mistaken belief about proper placement of registration sticker). While the court holds that  
6 probable cause is required to use CSS devices to pinpoint the location of a cell phone,  
7 the OPD and FBI’s reliance four years ago on the view that the pen register statute  
8 governed the use of the Stingrays, which were configured so as not to capture any  
9 content of communications, was not objectively unreasonable.

10 Where the OPD had applied for and obtained a search warrant for Ellis’s  
11 apartment before the Stingrays were deployed, and Officer Saunders applied for a pen  
12 register order that authorized wireless carriers to provide law enforcement with cell  
13 site/sector location information for Ellis’s phone, for which the issuing judge did not  
14 require a showing of probable cause, the OPD and FBI used the Stingrays in objectively  
15 reasonable reliance on the emergency provisions of the pen register statute and the pen  
16 register order. The court finds that the officers were acting “as a reasonable officer would  
17 and should act in similar circumstances,” such that “excluding the evidence can in no way  
18 affect [their] future conduct unless it is to make [them] less willing to do his duty,” so as to  
19 warrant the good faith reliance exception. *United States v. Crews*, 502 F.3d 1130, 1136  
20 n.4 (9th Cir. 2007) (citing *Leon*, 468 U.S. at 920) (internal marks omitted). Accordingly,  
21 the motion to suppress is DENIED on this additional ground.

## 22 2. Inevitable Discovery

23 The government also argues that under the inevitable discovery doctrine, Ellis  
24 undoubtedly would have been located by the OPD inside the apartment building, even  
25 without the use of the Stingray devices.

26 The inevitable discovery exception to the exclusionary rule permits the admission  
27 of otherwise excluded evidence “if the government can prove that the evidence would  
28 have been obtained inevitably and, therefore, would have been admitted regardless of

1 any overreaching by the police. . . .” *United States v. Reilly*, 224 F.3d 986, 994 (9th Cir.  
2 2000) (quoting *Nix v. Williams*, 467 U.S. 431, 447 (1984)). “If the prosecution can  
3 establish by a preponderance of the evidence that the information ultimately or inevitably  
4 would have been discovered by lawful means . . . then the deterrence rationale has so  
5 little basis that the evidence should be received.” *Nix*, 467 U.S. at 444.

6 Here, the evidence in the record reflects that police officers and SWAT members  
7 had established a perimeter around 1759 Seminary by at least 10:41 pm, according to  
8 the CAD reports, well before the first Stingray device was deployed. They had also sent  
9 in a robot and bean bags and instructed residents to stay away from the windows,  
10 believing that suspects were inside the building. While the cell phone location  
11 information obtained by the Stingrays facilitated locating Ellis in a specific apartment,  
12 under these circumstances, the police would have eventually found Ellis inside and  
13 apprehended him, even without the use of the Stingrays. See *United States v. Takai*,  
14 943 F. Supp. 2d 1315, 1324–25 (D. Utah 2013) (denying motion to suppress based on  
15 warrantless cellphone GPS pinging data from cellular providers pursuant to 18 U.S.C.  
16 § 2702(c)(4), where the defendant’s location was already being staked out and discovery  
17 was inevitable even absent the cellphone GPS pinging data).

18 Accordingly, the court finds that the inevitable discovery exception is a separate  
19 ground for DENYING the motion to suppress.

20 **E. Failure to Disclose Stingray in Pen Register Application**

21 Because the government relies on the pen register order to authorize the use of  
22 the Stingrays, Ellis requests a *Franks* hearing based on the affiant’s misleading  
23 omissions in the pen register application about the use of cell site simulators by the FBI  
24 and OPD. Doc. no. 304 at 22 (citing *Franks v. Delaware*, 438 U.S. 154 (1978)). Ellis  
25 argues that the officer failed to disclose to the state court judge that MetroPCS would not  
26 be conducting the surveillance, but that the FBI and OPD would each use Stingrays to  
27 locate Ellis’s phone. Ellis contends that the application fails to particularize the  
28 information to be collected from the Stingrays or from whom. *Id.* Ellis also argues that

1 the OPD and FBI deliberately misled the state court judge by omitting any reference to  
2 the use or capabilities of the Stingray devices in seeking the pen register order, and that  
3 a *Franks* hearing is warranted by the government's misleading statements to the court.

4 As discussed above with respect to good faith reliance on the pen register  
5 procedures, Officer Saunders's failure to explain that a Stingray device would be used by  
6 law enforcement to locate the cell phone did not amount to a knowingly false statement  
7 or reckless disregard for the truth, where such details of execution were not required to  
8 be specified under *Dalia*, 441 U.S. at 258. In *Patrick*, the Seventh Circuit rejected a  
9 defendant's challenge to the failure of the police to disclose in a location-tracking warrant  
10 application that they planned to use a cell-site simulator, implying that they would obtain  
11 location information from his cell phone company's data. *Patrick*, 842 F.3d at 544. The  
12 court in *Patrick* held that under *Dalia* and *Richards* (holding that no-knock entry in  
13 executing search warrant was reasonable under the circumstances even though the  
14 issuing judge denied the request for advance authorization for no-knock entry), "the  
15 police could have sought a warrant authorizing them to find [a suspect's] cell phone and  
16 kept silent about how they would do it." *Id.* The *Patrick* court reasoned that under the  
17 authority of *Dalia* and *Richards*, and other considerations, "the Fourth Amendment *forbids*  
18 judges to attempt to regulate, *ex ante*, how a search must be conducted, and confines  
19 the judiciary to *ex post* assessments of reasonableness." *Id.* at 544-45 (citing Orin S.  
20 Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va. L. Rev. 1241, 1260–  
21 71 (2010)). See also *United States v. Rigmaiden* ("*Rigmaiden III*"), 2013 WL 4525252, \*5  
22 (D. Ariz. Aug. 27, 2013) (denying motion for reconsideration of denial of suppression  
23 motion, rejecting arguments that the tracking warrant lacked particularity and that the  
24 government violated its duty of candor by failing to disclose additional technical details of  
25 the mobile tracking device used to locate the defendant's aircard, following *Dalia*).

26 In light of these authorities, the omitted references to the Stingray devices at issue  
27 do not demonstrate knowingly false statements or reckless omissions of material fact to  
28 the state court so as to warrant an evidentiary hearing. See *United States v. Stanert*, 762



1 F.2d 775, 781 (9th Cir.), *amended*, 769 F.2d 1410 (9th Cir. 1985) (requiring “that the  
2 defendant make a substantial showing that the affiant intentionally or recklessly omitted  
3 facts required to prevent technically true statements in the affidavit from being  
4 misleading” to warrant a hearing under *Franks*). Here, the pen register order authorized  
5 the OPD and FBI to obtain real-time information about cell site/sector location and signal  
6 direction and strength for Ellis’s phone, the purpose of which was to determine the  
7 location of Ellis’s cell phone. Doc. no. 304, Ex. I. Under *Dalia* and *Chen*, and the  
8 persuasive authority of *Patrick*, the OPD affiant was not required to disclose the use of  
9 the Stingray devices to determine Ellis’s cell phone location. Accordingly, Ellis has not  
10 demonstrated that a *Franks* hearing is warranted.

11 **F. Possibility of Interceptions in Violation of Title III**

12 Ellis contends that if the Stingrays used by OPD and the FBI captured content or  
13 were used as a microphone to pick up conversations, even if not recording or capturing  
14 them, then their use violated Title III of the Omnibus Crime Control and Safe Streets Act  
15 of 1968, 18 U.S.C. §§ 2510 et seq. Doc. no. 304 at 19-20. Title III requires an  
16 application for an order authorizing interception of a wire, oral, or electronic  
17 communication to establish probable cause to believe “that an individual is committing,  
18 has committed, or is about to commit a particular offense,” and probable cause to believe  
19 that “particular communications concerning that offense will be obtained” by intercepting  
20 communications over the targeted facilities. 18 U.S.C. § 2518(3). Each application and  
21 order must contain a “particular description of the type of communication sought to be  
22 intercepted.” 18 U.S.C. §§ 2518(1)(b)(iii) and (4)(c).

23 It is undisputed that neither the OPD nor FBI applied for an order for electronic  
24 surveillance under 18 U.S.C. § 2518, and that the state court order did not authorize  
25 interception of communications from the target phone. Ellis points out that cell site  
26 simulators are capable of intercepting conversations by using the target cell phone as a  
27 microphone, and suggests that there is evidence to suggest that the police were listening  
28 to conversations on his phone by using the Stingrays. See doc. no. 304, Ex. O

1 (USABook excerpt on electronic surveillance referring to the possibility of using Stingrays  
2 to “intercept conversations using a suspect’s cell phone as the bug”). Ellis cites the  
3 police radio recordings of officers discussing “some activity on the phone right now” and  
4 that “he’s live on his uh every couple minutes.” Doc. no. 304-1 (Boersch Decl.) ¶ 19.  
5 Ellis suggests that this evidence is inconsistent with the government’s representations  
6 that the Stingrays used in this case did not capture or collect content, but he merely  
7 speculates that the Stingrays were configured to intercept conversations through his cell  
8 phone. The police officers’ conversation about activity on the phone does not support an  
9 inference that the content of the conversations were being intercepted, particularly in light  
10 of the declarations by law enforcement officers who attested that the Stingrays did not  
11 obtain or collect content or communications from the target cell phone.

12 The unnamed OPD operator states in his declaration that the OPD’s cell site  
13 simulator (1) “was not configured to capture the content of any communications, including  
14 data contained on the phone itself;” (2) “does not remotely capture e-mails, texts, contact  
15 lists, images, or other data from the phone, nor does it, as configured, provide subscriber  
16 account information;” and (3) “[t]he device used to locate the defendant’s cell phone  
17 therefore did not capture, collect, decode, view or otherwise obtain any content  
18 transmitted from the defendant’s cell phone or any others in the area.” Doc. no. 321, Ex.  
19 G ¶ 8 and Ex. H.

20 Similarly, the unnamed FBI agent’s declaration indicates that “cell site simulators  
21 used by Federal, state, and local law enforcement must be configured as pen registers,  
22 and may not be used to collect the contents of any communication, in accordance with 18  
23 U.S.C. § 3127(3)[, including] any data contained on the phone itself.” Doc. no. 321, Ex. I  
24 ¶ 7. The FBI agent further states, “[t]he cell site simulator does not remotely capture e-  
25 mails, texts, contact lists, images, or other data from the phone, nor does it, as  
26 configured, provide subscriber account information (such as an account holder’s name,  
27 address, or telephone number).” *Id.* With respect to the use of the FBI cell site simulator  
28 on January 22, 2013, to locate Ellis’s cell phone, “it only obtained the signaling

1 information relating to that particular phone[;] such signaling information did not include  
2 content such as e-mails, texts, contact lists, images, or other data from the phone, nor did  
3 it provide subscriber account information.” *Id.* ¶ 11. The FBI agent attests that “[i]n line  
4 with general FBI policy and practice,” the cell site simulator equipment was not  
5 configured to collect (1) any content contained on or transmitted by the target device;  
6 (2) subscriber account information; or (3) voice or other audio communications from any  
7 device in the area, including the targeted device. *Id.* ¶ 13. *See also* doc. no. 321, Ex. J  
8 ¶ 7 (Decl. of FBI Program Manager).

9 The evidence in the record is sufficient to determine that the cell site simulators  
10 were not used to intercept conversations or other communications over cell phones in  
11 violation of Title III. *See United States v. Oliva*, 705 F.3d 390, 397-400 (9th Cir. 2012)  
12 (affirming denial of motion to suppress where defendant argued that orders authorizing  
13 government to intercept wire communications to and from certain target phones under  
14 Title III could have given the government broader authority to convert the targeted  
15 phones into roving bugs or roving wiretaps, where the government disavowed such  
16 surveillance). Ellis’s motion to suppress for violation of Title III is therefore DENIED.

## 17 **II. Ellis’s Motion to Suppress Evidence Seized from Apt. 212**

18 Ellis seeks suppression of evidence seized from his apartment, No. 212, on the  
19 ground that the government has failed to produce the original file-stamped search  
20 warrant and warrant affidavit, and has thereby failed to demonstrate that the search of  
21 Apartment 212 was conducted pursuant to a valid search warrant. Alternatively, Ellis  
22 seeks suppression of the evidence given the extraordinary delay from when the search  
23 was conducted and when the search warrant was returned and filed with the state court.  
24 Doc. no. 307.

### 25 **A. Lack of Original Warrant**

26 Although the defense has not previously moved to suppress the search warrant for  
27 lack of the original, the court has already addressed the validity of the search warrant for  
28 Apartments 108, 110 and 212 in denying defendants’ earlier motions to suppress.

1 10/29/15 Order. In brief, the court found that after police responded to the shooting of a  
2 police officer the evening of January 21, 2013, OPD secured the apartment complex and  
3 obtained a valid search warrant, supported by a showing of probable cause, to search  
4 Apartments 108, 110 and 212. Having reviewed the relevant evidence in the record,  
5 including the factual statements in the unredacted search warrant affidavit based on  
6 information provided by a confidential informant, filed under seal, the court determines  
7 that despite the absence of an original file-stamped warrant, the record is sufficient to  
8 determine that OPD conducted a search of Apartment 212 pursuant to a warrant. See  
9 Gov't Ex Parte Submission of Proposed Redactions to State Court Warrant Affidavits for  
10 In Camera Review (filed under seal November 12, 2014). Defense counsel's continued  
11 objections to the court's reliance on redacted information to determine the validity of the  
12 search warrants are overruled in light of the government's prior representations that the  
13 informant will not be called to testify and the redacted information will not be offered at  
14 trial to prove the charged conduct. See *McCray v. Illinois*, 386 U.S. 300, 311 (1967);  
15 *United States v. Fixen*, 780 F.2d 1434, 1439 (9th Cir. 1986).

16 Ellis also points out inconsistencies in the search inventory and police reports,  
17 doc. no. 307 at 15, such as Officer Milina's failure to list the three handguns from  
18 Apartment 212 in his report, Ex. Q, or the failure to list the handguns in the search  
19 inventory, Ex. G. The government responds that Milina's inventory does in fact refer to  
20 "Box w/ 3 glock pistols" and that his report explains that he gave the firearms to  
21 Technician Jaecksch, who documented them in her report, which explains the omission  
22 of the guns from Milina's property record, Ex. T. Doc. no. 322 at 9 (referring to Jaecksch  
23 report at Bates 3447).

24 Ellis further takes issue with the fact that the police left a blank search warrant in  
25 Apartment 212, which has no indication that portions were redacted, suggesting that  
26 Judge Horner may have signed a blank warrant which would be overbroad. Doc. no. 325  
27 at 3-4 and Reply Ex. A. This suggestion is purely speculative and unreasonable in light  
28 of the record. The government cites Officer Milina's declaration, filed in opposition to

1 Ellis's earlier suppression motion, stating that he left a redacted version of the warrant  
2 per OPD policy. Doc. no. 322 at 6-7 (citing doc. no. 95-4). The government also  
3 compares the copy of the unredacted warrant produced to defendants with the redacted  
4 copy left at the scene, and points out there are no discrepancies in Judge Horner's  
5 signature and date. Doc. no. 322 at 7. Even if the police had not provided Ellis with any  
6 copy of the warrant, suppression of evidence obtained pursuant to a valid search warrant  
7 would not be justified. *United States v. Hector*, 474 F.3d 1150, 1154-55 (9th Cir. 2007)  
8 ("On its face, the Fourth Amendment does not require that a copy of the warrant be  
9 served on the person whose premises are being searched.") (citing *United States v.*  
10 *Banks*, 540 U.S. 31, 35 (2003) ("The Fourth Amendment says nothing specific about  
11 formalities in exercising a warrant's authorization.")).

12 The government has demonstrated that the OPD and FBI applied for, and  
13 obtained, a search warrant for Apartment 212, as corroborated by the timeline of events  
14 and the warrants that were issued contemporaneously. The years-long delay in locating  
15 and filing the original warrant that was issued by the state court judge may raise concerns  
16 about clerical operations after the search was conducted, but does not weigh against a  
17 finding that the police searched Apartment 212 pursuant to a warrant. To the extent that  
18 Ellis challenges the failure to produce the original warrant, the lack of an original may  
19 impact admissibility of that document at trial, but does not so outweigh the evidence,  
20 demonstrating that a warrant was issued, as to require suppression of the fruits of the  
21 search. Under Ninth Circuit authority, "California courts uniformly recognize that statutory  
22 provisions covering the filing and return of a search warrant are ministerial in nature, the  
23 violation of which does not in itself invalidate an otherwise lawful search or require  
24 suppression of evidence seized thereby, at least in the absence of demonstrated  
25 prejudice to the defendant." *United States v. Towne*, 997 F.2d 537, 542 n.3 (9th Cir.  
26 1993) (where the court file was missing an attachment incorporated by reference in a  
27 search warrant, court may consider extrinsic evidence to determine if attachment  
28 accompanied warrant when search was authorized and carried out, and whether to treat

1 the missing attachment as part of the warrant). As defense counsel concedes, there is  
2 no state court authority requiring suppression as a remedy for failure to comply with the  
3 search warrant return procedures. *See People v. Head*, 30 Cal. App. 4th 954, 958 (1994)  
4 (“No California case has yet held that a late or otherwise faulty return violates the Fourth  
5 Amendment.”).

6 Accordingly, the fact that the original search warrant cannot be located in the state  
7 court record does not establish that the warrant was invalid or that the search of  
8 Apartment 212 was unreasonable. The motion to suppress the evidence seized from  
9 Apartment 212 for lack of the original search warrant is therefore DENIED.

10 **B. Prejudice from Delay**

11 In the alternative, Ellis contends that he has been prejudiced by the government’s  
12 delay of nearly four years in filing the return of the search warrant in state court, which  
13 has led to extensive litigation over producing the file-stamped warrant to determine its  
14 validity. He asserts that the delay has prejudiced all defendants by diverting time and  
15 resources to litigating the issue and by extending the length of their pretrial detention,  
16 particularly Ellis who has been in solitary confinement for most of that time. Ellis further  
17 argues that the delay raises uncertainty over the discrepancies in the copies of the  
18 search warrant and the police records related to the search, particularly given that  
19 defense counsel still cannot locate the original search warrant in the state court file.

20 The government accepts responsibility for the delay, almost three years after this  
21 case was commenced in December 2013, in realizing that the original search warrant  
22 and Ellis’s arrest warrant had not been returned to the state court until September 2016  
23 when they were discovered in the OPD’s files that were in the FBI’s custody. Doc. no.  
24 322 at 4.

25 Though the delay in locating the original file-stamped search warrant for  
26 Apartments 108, 110 and 212 is ongoing and is now approaching four years, Ellis has not  
27 demonstrated prejudice from this delay in light of the record. In November 2014, the  
28 court reviewed the search warrant affidavits in camera and approved certain redactions

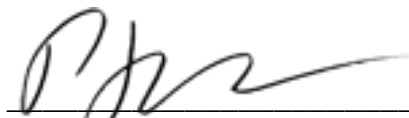
United States District Court  
Northern District of California

1 proposed by the government. The government represents that it produced a redacted  
2 copy of the search warrant affidavit for Apartment 212 in December 2014, and a copy of  
3 the warrant was subsequently produced in May 2015, after which the parties litigated  
4 defendants' pretrial motions, including motions to suppress. Doc. no. 322 at 2-3. Thus,  
5 defendants have had copies of the search warrant and redacted affidavit for over two  
6 years, enabling defendants to challenge the probable cause showing and prepare a  
7 defense. Ellis has not shown that the lack of the original search warrant has been so  
8 prejudicial as to merit suppression of the evidence. *See United States v. Motz*, 936 F.2d  
9 1021, 1025 (9th Cir. 1991) (suppression not warranted where the agents executed a valid  
10 search and the defendants "were not prejudiced by the agents' failure to perform the  
11 ministerial requirements" for return and inventory under Rule 41).

12 Accordingly, Ellis's motion to suppress evidence seized from Apartment 212 on  
13 the ground of prejudicial delay is DENIED.

14 **IT IS SO ORDERED.**

15 Dated: August 24, 2017



16  
17 PHYLLIS J. HAMILTON  
United States District Judge

18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28