BOERSCH SHAPIRO LLP
David W. Shapiro (State Bar No. 219265)
Dshapiro@boerschshapiro.com
Martha Boersch (State Bar No. 126569)
Mboersch@boerschshapiro.com
Lara Kollios (State Bar No. 235395)
Lkollios@boerschshapiro.com
1611 Telegraph Ave., Ste. 806
Oakland, CA 94612
Telephone: (415) 500-6640

Attorneys for Defendant
PURVIS LAMAR ELLIS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

UNITED STATES OF AMERICA, Plaintiff v. PURVIS LAMAR ELLIS, et al. Defendants.	Case No. CR-13-00818 PJH **ALL DEFENDANTS NOTICE OF MOTION; MOTION TO SUPPRESS EVIDENCE OBTAINED FROM STINGRAY AND FOR *FRANKS* HEARING; AND MEMORANDUM IN SUPPORT** Hearing Date: June 14, 2017 Hearing Time: 1:30 p.m. Trial Date: TBD

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

NOTICE OF MOTION

TO: UNITED STATES OF AMERICA, PLAINTIFF; BRIAN STRETCH, ACTING UNITED STATES ATTORNEY; AND JOSEPH ALIOTO, ASSISTANT UNITED STATES ATTORNEY:

PLEASE TAKE NOTICE that on June 14, 2017, at 1:30 p.m. or as soon thereafter as the matter may be heard, in the courtroom of the Honorable Phyllis Hamilton, United States District Judge, all defendants, by and through undersigned counsel of record for Purvis Ellis, will move this Honorable Court for an order suppressing all evidence obtained through the use of a Stingray as well as all fruits of that search, and a *Franks* hearing regarding the same. This motion is based upon the Fourth Amendment to the United States Constitution, the attached Memorandum, the Declaration of Martha Boersch, all files and records in this case, and any further evidence as may be adduced at the hearing on this Motion.

MEMORANDUM OF POINTS AND AUTHORITIES

INTRODUCTION

The defendants move to suppress any and all evidence obtained or derived from the use of any cell-site simulators in this case, and/or for a *Franks* hearing.[1]

The defendants have been in pretrial custody for more than three years while the government has repeatedly delayed production of relevant discovery. For more than a year after the defendants were indicted, defense counsel repeatedly asked the government to confirm the use of any electronic surveillance. The government ignored those requests, leaving the defense no choice but to file a motion in February 2015 to compel that information. The reason for the government's silence became apparent when, in response to the motion, the government finally admitted that *a* Stingray had been used. Dkt. 93 at 2 ("the United States confirms that *a* cell-site simulator was used in this case to obtain the general location of an armed suspect at large." (emphasis added).)

[1] "A cell-site simulator—sometimes referred to as a 'StingRay,' 'Hailstorm,' or 'TriggerFish' – is a device that locates cell phones by mimicking the service provider's cell tower (or 'cell site') and forcing cell phones to transmit 'pings' to the simulator." *United States v. Lambis*, 197 F.Supp. 3d 606, 609 (S.D.N.Y. July 12, 2016). The defense shall refer to the cell-site simulators as "Stingrays" in this motion.

But the government's obfuscation continued when it persisted in denying that more than one Stingray had been used. At an August 5, 2015 status conference, counsel for the defense attempted to explain to the Court why the defense believed that multiple Stingrays were used. The government accused the defense of baseless conjecture and affirmatively asserted that only one Stingray was used, by the FBI: "I can say right now almost definitively that there were not two cell-site simulators used. And all of the conjecture that you have just recently heard is just nothing more than conjecture." Boersch Decl. Ex. A. But as we now know, there *were* two Stingrays used, one by the FBI and one by the Oakland Police Department ("OPD"). And although the government ultimately admitted to using two Stingrays, after over a year of denial, it still refuses to provide necessary information about its Stingray policies and guidelines, including but not limited to whether the Stingrays were configured to capture content (*i.e.*, text messages, phone conversations, *etc*.) or to act as a microphone.[2]

The government's opacity on its use of the Stingrays is not unique to this case or this District. Just six months ago, the Honorable Chief Judge Diane Wood of the Seventh Circuit said this about the government's efforts to hide information regarding its use of Stingrays:

> This is the first court of appeals case to discuss the use of a cell-site simulator, trade name "Stingray." We know very little about the device, thanks mostly to the government's refusal to divulge any information about it. Until recently, the government has gone so far as to dismiss cases and withdraw evidence rather than reveal that the technology was used. See Memorandum Agreement between Amy S. Hess, Assistant Director, Operational Technology Division, FBI, and David Salazar, Chief of Police, MPD (Aug. 13, 2013) (agreeing to dismiss cases rather than disclose use of Stingray).

United States v. Patrick, 842 F.3d 540, 546 (7th Cir. 2016) (Wood, Chief J., dissenting).

In the present case, neither the FBI nor the OPD obtained search warrants or lawful court orders before deploying the two Stingrays. The use of those Stingrays constituted a search under the Fourth Amendment that required search warrants, and the court order for a pen register the government obtained was obtained through deception and falsehoods. All evidence derived from the

[2] The defense will again meet and confer with the government regarding those items and file a motion to compel should the government continue to refuse to produce them.

use of the Stingrays must therefore be suppressed. *See United States v. Lambis*, 197 F.Supp. 3d 606 (S.D.N.Y. 2016) (suppressing all evidence, including drugs and drug paraphernalia, seized from the defendant's apartment because the search stemmed from the government's illegal use of a Stingray).

STINGRAY SURVEILLANCE TECHNOLOGY

The defense has previously described for this Court the technology of cell-site simulators and incorporates that briefing here. *See* Dkt. 118 at 7-10. For purposes of this motion to suppress, these are the salient features of Stingray technology:

- A Stingray operates using electronic signals that penetrate walls and physical barriers that protect homes, offices, and other private places;
- A Stingray masquerades as a cell phone tower, forcing *all* wireless devices within range to communicate with it, whether those devices are targeted or not;
- From those forced communications, a Stingray can identify all phones within range, and can forcibly obtain from those phones information including phone numbers, IMSI, IMEI, and TMSI information;[3]
- A Stingray can pinpoint the precise location of a phone within constitutionally protected spaces with an accuracy of two meters;
- A Stingray can intercept content transmitted from phones within its range;
- A Stingray can force a phone to act as a microphone, essentially converting the phone to a wiretap;
- A Stingray operates independently of any wireless carrier.[4]

[3] IMSI: acronym meaning "International Mobile Subscriber Identity," a unique identifier for a user of a mobile network. The IMSI is stored in the SIM card for those phones using GSM networks, and within the phone or the R-UIM card for phones using CDMA networks. IMEI: acronym meaning "International Mobile Equipment Number," a unique identifier number tied with the specific mobile phone device connected to the network, almost like a serial number for the specific phone. TMSI: acronym meaning "Temporary Mobile Subscriber Identity," a unique identifier number ascribed temporarily to a specific mobile device by the network to which the device is connected. *See* Adrian Dabrowski, et al, IMSI-Catch Me If You Can: IMSI-Catcher-Catchers, in Annual Computer Security Applications Conference (ACSAC)(2014) at 2.

[4] In its October 26, 2016, letter, the government claimed that "[n]o content, conversations, or text messages were captured, so there are no records documenting any such content. The cell-site simulator intercepted and temporarily collected the dialing, routing, addressing and signaling

The Department of Justice has described Stingray technology as follows:

> Cell-site simulators ... function by transmitting as a cell tower. In response to the signals emitted by the simulator, cellular devices in the proximity of the device identify the simulator as the most attractive cell tower in the area and thus transmit signals to the simulator that identify the device in the same way that they would with a networked tower.
>
> A cell-site simulator receives and uses an industry standard unique identifying number assigned by a device manufacturer or cellular network provider. When used to locate a known cellular device, a cell-site simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the cell-site simulator identifies the specific cellular device for which it is looking, it will obtain the signaling information relating only to that particular phone. When used to identify an unknown device, the cell-site simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.
>
> By transmitting as a cell tower, cell-site simulators acquire the identifying information from cellular devices. This identifying information is limited, however. Cell-site simulators provide only the relative signal strength and general direction of a subject cellular telephone; they do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications. Moreover, cell-site simulators used by the Department must be configured as pen registers, and may not be used to collect the contents of any communication, in accordance with 18 U.S.C. § 3127(3). This includes any data contained on the phone itself: the simulator does not remotely capture emails, texts, contact lists, images or any other data from the phone. In addition, Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number).

---

information of the target phone in order to determine its approximate location. It did not collect any phone numbers." However, DOJs own Electronic Surveillance Manual makes clear that, at the very least, a cell site simulator will capture phone numbers when a target phone is used to make or receive a call. Boersch DecL., Ex. B ("If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/ triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected"). The CAD reports suggest that this is exactly what OPD was doing. For example, at one point the following exchange occurred between two officers early on the morning of January 22, 2013:

> Porter, this Omega, I was told there's some activity on the phone right now, because of 108 maybe.
> Yeah Omega, he's uh, he's live on his uh every couple minutes.

Boersch Decl. ¶19 (PHOTOS-VIDEOS-000035, Disc 3 Track 2 at 4:30).

United States v. Patrick, 842 F.3d 540, 542-43 (7th Cir. 2016) (quoting Department of Justice Policy Guidance: Use of Cell–Site Simulator Technology (Sept. 3, 2015) at 2.).

STATEMENT OF FACTS

I. PROCEDURAL HISTORY RELATING TO THE STINGRAYS

A. Background

Defendant Purvis Ellis and his three co-defendants were indicted by a federal grand jury on December 19, 2013, for conspiracy to violate RICO and several other offenses arising from two incidents on January 20 and 21, 2013. On January 20, 2013, an individual was shot on Foothill Boulevard in Oakland, and on January 21, 2013, an undercover police officer who had entered the rear parking lot of an apartment building on Seminary Avenue was shot in the wrist. According to discovery produced to the defense, Ellis has never been identified as involved in the shooting of the officer and is not substantively charged with that offense. Defendant Ellis was allegedly identified as the driver of a car on January 20 that picked up two suspects after the shooting.

Ellis was originally charged in state court with offenses arising from the January 21, 2013 incident. Those charges were dismissed, however, after Ellis's defense counsel asked the Alameda County District Attorney to produce the search warrant affidavits that led to Ellis's arrest on those charges. Boersch Decl., ¶2. Those search warrant affidavits were never produced in the state proceedings. Instead, this federal indictment followed.

B. The Defense Requests for Disclosure of Electronic Surveillance

The defendants have made numerous requests for disclosure of electronic surveillance and evidence related to that surveillance. On May 28, 2014 – three years ago – defense counsel made the following specific request related to electronic surveillance:

> 18. The disclosure of any electronic video or surreptitious interception or recording which was made of any conversation or activity in connection with this case. This Request includes, but is not limited to,
>
> a. production of any memoranda, transcripts, notes or other record thereof, preserved by any means whatsoever, which were procured by any electronic, mechanical, or physical wiretapping, eavesdropping, overhearing, or surveillance;
>
> b. the circumstances under which such surveillance or eavesdropping

was conducted; and

c. copies of any written orders, applications for orders, or memoranda to obtain permission to intercept communications from any executive or judicial authority.

19. A copy of all telephone toll records reviewed in connection with this case by any government agents or attorneys, or by any other persons working in conjunction with such agents, and copies of all applications, orders, or subpoenas prepared in connection with the obtaining of such telephone toll records.

20. All call data obtained in this case, all phone numbers obtained/monitored in the course of this investigation, and all cell-site data obtained during the investigation.

21. Full documentation of the sources of all call record data collected by the government (including the Oakland Police Department and the Northern California HIDTA Task Force) in this case, including data obtained (directly or indirectly) from cell phone service providers, the National Security Agency, the DEA Special Operations Division, the Hemisphere Project, the Northern California Regional Intelligence Center, or any other such government intelligence agency or task force group.

22. Any and all communications between law enforcement and/or Department of Justice officials involved with this case and the Hemisphere Project, the Northern California Regional Intelligence Center, or the DEA Special Operations Division, regarding the collection of cell phone call record data in the investigation of this case.

23. All call data, telephone toll records, GPS, and cell site data for

a. Any cell phone used by Officer Eric Karsseboom including his personal and/or Oakland Police Department issued cell phone from January 21, 2013 through March 1, 2013.

b. Any cell phone used by Officer Malcolm Miller including his personal and/or Oakland Police Department issued cell phone from January 21, 2013 through March 1, 2013.

Boersch Decl., Ex. C.

C. The Government's Initial Disclosure That *A* Stingray was Used Without a Warrant And Denial That any Other Cell-Site Simulator was Used

The government never responded to defense counsel's specific requests for disclosure of information related to electronic surveillance. Therefore, on February 6, 2015, defense counsel filed a "Motion for Search and Disclosure of Electronic Surveillance" pursuant to 18 U.S.C. § 3504(a), which provides that the United States "shall affirm or deny" the use of electronic surveillance. Dkt.

78. The government's response to the motion was cryptic, and, as we now know, misleading: "the United States confirms that *a* cell-site simulator was used in this case to obtain the location of an armed suspect at large." United States' Response to Defendants' Motion for Disclosure of Electronic Surveillance, Dkt. 93 at 2 (emphasis added). The government's response did not indicate whether the cell-site simulator was used by the FBI or the OPD, it did not identify the "armed suspect" or the evidence sufficient to believe that the target of the simulator was either armed or a suspect, and it did not describe exactly what technology was used or what information was obtained or reviewed.

The government also stated in its response that OPD "sought cell phone records" without a warrant, ostensibly based on exigent circumstances. *Id*. at 3. The government then referenced two documents executed by OPD that had been attached to the defense motion: a "Metro PCS CALEA Pen and Wiretap Worksheet" for 661-862-0279, and a Metro PCS "Exigent Circumstance Request" for 510-904-7509, which was allegedly executed at 23:15 on January 21, 2013. Boersch Decl., Exs. D and E. The latter document specifically required: "All requests for cells site locations MUST be followed-up by a legal document signed by a judge within 48 business hours." Boersch Decl., Ex. E (emphasis in original). The government did not provide any "legal document" or any further information. The government has never explained how or why it focused on these two phone numbers, except that it contends the second number belonged to Ellis. As noted, the government has never provided any evidence to justify its focus on Ellis's phone number: the discovery produced to the defense shows that Ellis was not identified as involved in the shooting on January 21.[5]

After the defendants filed a reply brief arguing that the warrantless use of a cell-site simulator violated their Fourth Amendment rights and seeking further information about the device, the Court allowed the government to file a brief in response. In that brief, the government asserted that it was continuing to search for other relevant discovery, and claimed, erroneously, that "the defense did not send any discovery requests before filing their motion." Dkt. 120 at 2.

On May 26, 2015, after a status conference, defense counsel sent another letter to the government specifically requesting the following:

[5] The government has not produced any witness statements and the search warrant affidavits are heavily redacted.

1. Please identify the name of the "armed suspect at large."

2. Identify any and all cell phones and/or cell phone numbers that were intercepted or tracked by the cell-site simulator;

3. Identify the type of information intercepted by the cell-site simulator, e.g., whether location or contents and if contents whether text messages, emails, phone calls or any other form of content;

4. Provide any and all evidence and records – whether written, audio, digital or in whatever form – obtained or reviewed as a result of the use of the cell-site simulator;

5. Provide any and all applications, requests, warrants, affidavits, notifications, or orders related to the use of the cell-site simulator in this case and/or which purport to seek the authorization or authorize the use of the cell-site simulator;

6. Provide copies of any and all agreements between the Oakland Police Department and any federal agency, including the Department of Justice, the United States Attorney's Office, the Federal Bureau of Investigation, or the Federal Communications Commission, relating to the use of any cell-site simulator, including, but not limited to, any non-disclosure agreement executed by the Oakland Police Department or any state or local law enforcement agency involved in the investigation of this matter as a condition of receiving the cell-site simulator equipment or technology.

Boersch Decl., Ex. F. The defense received no response. In June 2015, in further briefing on the Stingray issues and in view of the substantial delays in the production of discovery, the defendants filed a brief requesting that the Court order the government to produce all records relating to electronic surveillance within 14 days.

On August 4, 2015, three months later and one day before a scheduled hearing, the government finally responded to the defense letter:

> I have confirmed through our investigative agency that on January 22, 2013, the FBI used a cell-site simulator to track the phone associated with Purvis Ellis, (510) 904-7509, who was a suspect in the shooting of an Oakland police officer hours earlier. The cell-site simulator intercepted and temporarily collected the dialing, routing, addressing, and signaling information of the target phone in order to determine its approximate location. It did not collect any GPS location information. It did not collect any phone numbers. It did not collect any content, including text messages, emails, phone calls or any other form of content. *The information collected from the cell-site simulator was purged after Mr. Ellis was arrested.*

Boersch Decl., Ex. G (emphasis added).[6] The letter did not specify whether this FBI use of a cell-site simulator was the use the government referenced in its response to the defense motion for disclosure of electronic surveillance. Nor did the letter describe the specific technology used or explain the basis for the government's belief that the phone number was "associated with Purvis Ellis."

Attached to this August 4 letter, the government produced, *for the first time* and more than a year after the defendants' specific request, an *FBI* "Exigent Request" for pen register information directed to "Metro PCS, AT&T Wireless Services, Nextel Communications, Spring PCS, Cricket Communications, Cingular Wireless, MCI Worldcomm, Sure West Wireless, T-Mobile, Voice Stream Wireless, Citizens Utilities, Pacific Bell Telephone Company, SBC Communications and any other affected telecommunication companies, subsidiaries, or entities" and a "state court order providing for the use of the pen register to track the phone at issue." Boersch Decl., Exs. H and I. The FBI "Exigent Circumstances" request was made by the FBI at 7:30 am on January 22, 2013, and sought "subscriber data and pen register or Title III intercept."[7] The letter did not indicate whether the government considered this document responsive to the defense request for any order authorizing the use of a cell-site simulator.

The state court order, which is *not file-stamped*[8] but was allegedly signed at some unknown time on January 22, 2013, was an order allowing the use of a device described as "pen register and trap and trace device" on 510-904-7509. *Id.* at 1. The order ostensibly was issued under the authority of 18 U.S.C. § 2703(c) and (d). The order allowed the installation and use of a pen register

[6] The government has never specified the technology that was used, and different cell-site simulators have different capabilities. *See* Linda Lye, *Stingrays: The Most Common Surveillance Tool the Government Won't Tell You About, A Guide for Criminal Defense Attorneys*, ACLU of Northern California 1-3 (2014) (available at https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About_0.pdf) (hereinafter "Lye, *Stingrays*").

[7] In another example of the government's abuse of its ability to withhold information from the defense, it has redacted the name of the FBI agent who applied for the pen register. There can be no legitimate basis for this redaction.

[8] The defense has repeatedly asked the government for file-stamped copies of all search warrants, affidavits and orders related to any electronic surveillance or searches because, for instance, the purported search warrant for apartment 212, like the recently produced order for a pen register, is not file-stamped so there is no way to confirm from the document when it was executed or whether it was ever filed with any court.

and trap and trace device by the service provider:

> to register numbers dialed or pulsed from the Target Telephone number (510) 904-7509, to record the date and time of such dialing or pulsing, to record the length of the time the telephone receiver is off the hook for incoming or outgoing calls, and to receive cell site and/or location sites, for a period of thirty (30) days.

Boersch Decl., Ex. I at 1. The order says nothing about the use of a Stingray, cell-site simulator, or any equivalent technology.

Attached to the order was an application submitted *by the OPD, not by the FBI*, which is heavily redacted and which repeated the information also set forth in the heavily redacted search warrant affidavits, information that has never been provided to the defense.[9] The application did not mention the use of a Stingray, cell site simulator, or any equivalent device. The government again did not indicate whether it considered this order to be responsive to defense request, above, and did not respond to any of the other specific requests made in the defense May 26 letter.

Based on the information described above and the evidence that had been produced in discovery, the defense believed that the government was withholding information that at least two Stingrays had been used, but the government denied it. On August 5, 2015, at the hearing on the various motions, counsel for the government stated: "I can say right now almost definitively that there were *not* two cell-site simulators used. And all of the conjecture that you have just heard is nothing but conjecture." Dkt.129 at 41:11-14 (emphasis added). At the hearing, the Court ordered the defense to meet and confer with the government regarding outstanding discovery requests related to the use of electronic surveillance. *Id*. at 42-43.

On August 12, 2015, in response to the government's August 4 letter and the Court's admonition, the defense made a further request for discovery based on information the government

[9] The defense continues to object to the government's heavy reliance in this case on "secret" *ex parte* submissions and again asks that the information that has been redacted be disclosed to the defense as a matter of due process. There is no reason the information could not be provided to defense counsel. The government's use of secret submissions not only deprives the defendants of their Fifth and Sixth Amendment right to due process and effective assistance of counsel, but also run the risk of tainting the objectivity of the Court and creating bias against the defendants. *See, e.g.*, *United States v. Barnwell*, 477 F.3d 844, 850-51 (6th Cir. 2007) (stating that "[a]n *ex parte* communication between the prosecution and the trial judge can only be 'justified and allowed by compelling state interest.' . . . . The Government bears a heavy burden in showing that the defendant was not prejudiced when his counsel was excluded from these communications." (footnote and citations omitted).

had by now disclosed. Boersch Decl., Ex. J.

On August 17, 2015, this Court issued a written order on various motions and denied as moot the defense motion for disclosure of electronic surveillance, and ordered the parties to meet and confer on the defendants' further discovery requests and the government to "complete production responsive to those requests within 60 days of the hearing, unless the parties agree to a later date." Dkt. 127 at 23.

D. The Government Finally Admits That *Two* Stingrays Were Used Without Warrants, but Declines to Disclose Evidence Related to the Stingrays

On October 26, 2015, after a meet and confer between defense and government counsel, the government responded by letter to the defense discovery requests. Boersch Dec., Ex. K. In that letter, the government disclosed, for the first time, that indeed *two* cell site simulators were used – one by the FBI, the use of which the government had disclosed on August 4, 2015, and another by OPD, the use of which the government had not previously disclosed. The government also stated that OPD used a pen register "during the course of the evening of the incident and perhaps the next morning." *Id.* The government declined to provide any further discovery in response to the majority of the defense requests for information, citing the law enforcement privilege. In several subsequent meet-and-confer sessions, the government continued to refuse to disclose any further evidence about the use of the cell-site simulators and told the defense to file a motion.

In December 2015, the Court referred the discovery disputes, including the Stingray issues, to the Honorable Donna M. Ryu for a discovery conference. Dkt. 147. Over the next six months, the defense engaged in several meet-and-confers with the government and submitted a number of briefs to the Court in an effort to get the government to disclose material information related to the Stingrays and other issues. Ultimately, Magistrate Ryu ordered the government to submit, by August 22, 2016, declarations based on personal knowledge regarding the use of the two Stingrays.

II. THE EVIDENCE REGARDING THE USE OF THE STINGRAYS

On August 22, 2016, the government submitted a declaration from an FBI agent and one from an OPD officer. Dkts. 225-1 and 225-2. According to those declarations, OPD deployed a cell site simulator on the evening of January 21 to locate the cell phone with number 510-904-7509, which the

OPD officer "understood belonged to defendant Purvis Ellis" (Dkt. 225-2 ¶ 8), and the FBI deployed its Stingray the next morning (Dkt. 225-1 ¶ 8). The government has never explained to the defense or the Court why Ellis's phone was targeted or why OPD believed that phone number 510-904-7509 belonged to Ellis.

A. The OPD Stingray

According to the OPD officer's declaration, the OPD deployed a Stingray to 1759 Seminary around two hours after 6:40 p.m. on January 21, 2013. Dkt. 225-2 ¶ 10. "Sometime after midnight," the officer "powered on and began operating the cell site simulator." *Id.* ¶ 11. Before powering on the Stingray sometime after midnight, OPD contacted the telephone carrier and filled out "an exigent circumstances request to obtain pen register information/trap trace and subscriber information for phone number 510-904-7509 to assist in locating the cellular telephone with the cell site simulator." The OPD officer claims he did not begin operating the Stingray until after receiving "this information from the telephone provider."

At some point later that morning, OPD requested FBI assistance in locating Ellis's phone. Dkt. 225-2 ¶ 13. The declarant does not indicate why OPD needed FBI assistance or when the request for assistance was made. At around 10:00 a.m. on January 22, OPD shut down its Stingray and the FBI began operating their device. *Id.* At that point, the declarant claims that OPD purged all the information it had collected. *Id.* ¶ 15.

B. The FBI Stingray

The FBI declarant states that at approximately 7:00 a.m. on January 22, he received a request from an FBI agent in Oakland indicating that OPD was "requesting FBI assistance in the use of its cell site simulator." Dkt. 225-1 ¶ 8. The declarant then contacted the carrier for the "subject cellular telephone" and filled out an exigent circumstances request to get pen register/trap trace and subscriber information, including MIN, for phone number 510-904-7509 "to assist in locating the cellular telephone in conjunction with the cell site simulator." *Id.* ¶ 9. But the request form produced to the defense makes no reference to a Stingray and there was no court order obtained pursuant to this request. The declarant states that he "simultaneously requested FBI approval to deploy the cell site simulator in support of" OPD. *Id.* The declarant states that he turned on the FBI Stingray at 10:00

a.m. on January 22 and that once it was turned on it "detected the presence of the subject cellular phone." *Id.* ¶¶ 10 & 11.

The discovery produced to the defense suggests that the FBI Stingray was in use much earlier. According to that discovery, one Stingray, likely the FBI's, was apparently on its way to the scene by around 1:00 am on January 22, and "paperwork" was "pretty much done," according to radio broadcasts. *See* Boersch Decl., ¶20 (PHOTOS-VIDEOS-000028, Disc 3, Track 1 at 2:40) (an officer states "our friends that we have been talking to with the toy – what's the ETA?" and another responds that the last he checked it would be 45 minutes to an hour. Another officer then states "that's for the equipment to be here – I don't know about paperwork that has to go with it," and the first officer responds, "that's pretty much done"); *see also id.* at Ex. M (this radio broadcast happened just before the 00:56 line in the CAD about "SUBJ/BLK DOO RAG NO SHI BLU JNS JUST WALKED UP FRM CAR ON STREET"); *see also* Dkt. 118 at 1 n.2. At 2:56 am, Officer Crum reported "activity on phone related to [apartment] 108" but it is not clear what phone was "active," what device made that determination, or what the "activity" was. Dkt. 118, Ex. C. According to the CAD report, at 5:21 the morning of January 22 OPD had a "lock" on the phone, but again it is not clear what phone or what device was used. Dkt. 78, Ex. A.

The declarant further states that at some point, "in an effort to reduce the error radius and increase the accuracy of the location of the cellular telephone, a cell site simulator augmentation device was deployed into the interior of the apartment building." Dk. 225-1, ¶ 12. The government does not explain what this device is, why it was necessary, where in the apartment building it went, or how it got in there. Confusingly, the declarant then states that "[a]t all times during the deployment of the cell site simulator and the augmentation device, the equipment and I were located in a publicly accessible areas in and around the target apartment building." *Id.*

At approximately 11:00 a.m., the FBI deleted or purged "all data for this incident . . . once [it] learned that the subject was arrested and in custody." The declarant does not identify the suspect.

C. The Exigent Circumstances Requests for Pen Registers

At 2:11 a.m. on January 22, 2013, "MetroPCS CALEA Pen and Wiretap Worksheet" for phone number 510-904-7509 was faxed from OPD Officer Jason Saunders to Metro PCS seeking

"call data records from 1-10-13 until 1-21-13 and start pen register if phone is active and being used." *See* Boersch Decl., Ex. N. That document makes *no reference* to a cell site simulator nor does it provided any probable cause or even reasonable suspicion for the requested information and there is no court order accompanying the faxed request, even though the request asserts that the "court order" authorizes the disclosure of information including cell site location. *Id.* At 2:29 am on January 22, 2013, an exigent circumstances request for phone number 510-904-7509 was faxed from Metro PCS to someone (the name is illegible). Dkt. 89-4. At 2:45 am, Officer Saunders faxed a pen and wiretap worksheet for number 661-682-0279 to Metro PCS. Dkt. 89-3. Neither of these documents makes any reference to a Stingray. Five hours later, at approximately 7:30 am, the FBI executes an exigent circumstances request to Metro PCS for phone number 510-904-7509. Boersch Decl. Ex. H.

At some unknown time, allegedly on January 22, 2013, State Superior Court Judge Horner signed a court order for a pen register and trap and trace device on phone number 510-904-7509. The government suggests that the court order is related to the CALEA worksheet Officer Saunders faxed at 2:11 am on January 22, 2013. But the court order is not file-stamped so it is impossible to tell when it was signed or whether it was ever filed. In any event, the court order does not refer to or authorize the use of a Stingray.

Phone records relating to phone number 510-904-7509 were produced, although it is not clear when or pursuant to what request. PhoneRecords-00001-00002.

ARGUMENT

I. THE WARRANTLESS USE OF THE STINGRAYS VIOLATED THE FOURTH AMENDMENT

The Fourth Amendment of the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Warrantless searches are presumptively unreasonable. *Kyllo v. United States*, 533 U.S. 27, 32 (2001); *Lambis*, 197 F.Supp. 3d at 609. A warrant must be based on probable cause and must be specific as to the place searched and persons and things seized. If a warrant violates either of these

requirements, it violates an individual's constitutional rights.

The government's warrantless uses of the Stingrays in this case were unlawful, unreasonable searches in violation of the Fourth Amendment and all evidence obtained or derived from those searches must be suppressed.

A. The Use of the Stingrays was a Search Requiring a Warrant

The government's use of the Stingrays to monitor and track Ellis's phone – and/or any of the dozens of phones that were monitored – was a search under the Fourth Amendment requiring a warrant because the Stingrays emitted signals that penetrated the walls of Ellis's and others' private dwellings that were not open to visual surveillance. Such use of technology constitutes a search under the Fourth Amendment requiring a warrant. *United States v. Karo,* 468 U.S. 705, 714 (1984) (the monitoring of a beeper in a private residence, not open to visual surveillance, "violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence"); *see also, id.* at 715 (there is a Fourth Amendment violation when "without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage" of a residence). As the Supreme Court reiterated in *Kyllo,* "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' . . . constitutes a search – at least where the technology is not in general public use." 533 U.S. at 33 (citation omitted).

Even if the monitored phones were not physically within a residence, the use of the Stingrays was still a search under the Fourth Amendment because the individuals whose communications were monitored or intercepted had a privacy interest in the use and location of their phones. *Katz v. United* States, 389 U.S. 347, 361 (1967) (Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable (Harlan, J., concurring)); *Riley v. California,* 134 S. Ct. 2473, 2489-92 (2014) (discussing the privacy interests in the data on modern smart phones).

Furthermore, because a Stingray emits signals that penetrate the walls of constitutionally protected spaces, it essentially trespasses and, therefore, its use constitutes a search which, unless

authorized by a warrant, violates the Fourth Amendment. *See Silverman v. United States*, 365 U.S. 505 (1961) (insertion of spike mike into the walls of a home without a warrant violated the Fourth Amendment); *United States v. Jones*, 565 U.S. 400 (2012) (warrantless installation of GPS device on a car violated the Fourth Amendment). Finally, because the Stingray can track an individual's every move with an accuracy of about two meters, including within private homes, its use again constitutes a search and requires a warrant. *See Jones*, 565 U.S. at 415 (because GPS device generated "a precise, comprehensive record of a person's public movements" its use infringed upon reasonable expectation of privacy (Sotomayor, J., concurring)).

In *United States v. Lambis*, 197 F.Supp. at 608-09, the DEA obtained a warrant for pen register information and cell site location information ("CSLI") for a target cell phone. As described by the court, pen register information, which is a record from the service provider of the telephone numbers dialed from a specific phone, while "CSLI is a record of non-content-based location information from the service provider derived from 'pings' sent to cell sites by a target cell phone. CSLI allows the target phone's location to be approximated by providing a record of where the phone has been used." *Id.* Using the CSLI, the DEA was able to locate the general area in which the target phone was being used but could not "identify 'the specific apartment building,' much less the specific unit in the apartment complexes in the area." *Id.* at 609. To do that, the DEA deployed a Stingray and, using that technology, identified the apartment building and the specific apartment in which the target phone was located. *Id.* After obtaining consent from the occupants, the DEA searched the apartment and discovered drugs and drug paraphernalia. *Id.*

Granting the defendant's motion to suppress that evidence, the court held as follows:

> [T]he DEA's use of the cellsite simulator to locate Lambis's apartment was an unreasonable search because the "pings" from Lambis's cell phone to the nearest cell site were not readily available "to anyone who wanted to look" without the use of a cell-site simulator. *See United States v. Knotts*, 460 U.S. 276, 281, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983); *see also State v. Andrews*, 227 Md.App. 350, 395–96, 134 A.3d 324 (2016) (holding that the use of a cell site simulator requires a search warrant based on probable cause, and finding that the trial court properly suppressed evidence obtained through the use of the cell-site simulator). The DEA's use of the cell-site simulator revealed "details of the home that would previously have been unknowable without physical

> intrusion," *Kyllo*, 533 U.S. at 40, 121 S.Ct. 2038, namely, that the target cell phone was located within Lambis's apartment. Moreover, the cell-site simulator is not a device "in general public use." *Kyllo*, 533 U.S. at 40.

Id. at 610. The court further recognized that the DOJ now prohibits the use of a Stingray without first obtaining a warrant.

> Absent a search warrant, the Government may not turn a citizen's cell phone into a tracking device. Perhaps recognizing this, the Department of Justice changed its internal policies, and now requires government agents to obtain a warrant before utilizing a cell-site simulator. See Office of the Deputy Attorney General, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, 2015 WL 5159600 (Sept. 3, 2015); Deputy Assistant Attorney General Richard Downing Testifies Before House Oversight and Government Reform Committee at Hearing on Geolocation Technology and Privacy, 2016 WL 806338 (Mar. 2, 2016) ("The Department recognizes that the collection of precise location information in real time implicates different privacy interests than less precise information generated by a provider for its business purposes.").

Id. at 611.

B. The Warrantless Use of Stingrays Violated the Fourth Amendment

1. There was no Warrant

Neither OPD nor the FBI obtained a search warrant permitting either agency to use a Stingray or any similar technology to monitor Ellis's or anyone else's phone.

2. The Pen Register Order Did Not Authorize the Use of the Stingrays

The government may contend that the unfiled order signed by Judge Horner was legally sufficient to authorize the use of both of the Stingrays here. The government would be wrong.

First, as noted, the use of a Stingray requires a warrant, not a pen register order under Section 2703.

Second, even if under some circumstances an order under Section 2703 could lawfully authorize the use of a Stingray, this order certainly did not. The order instead requires a list of cell phone carriers to implement the "installation and use of pen register, to register numbers dialed or pulsed from the Target Telephone number (510) 904-7509, to record the date and time of such dialing or pulsing, to record the length of time the receiver is off the hook for incoming or outgoing calls, and

to receive cell site and/or location sites." Boersch Decl., Ex. I. The order did not allow the FBI or OPD to bypass the carriers and independently use a roaming cell-site simulator, which, as discussed above, performs very different and more intrusive functions than these. In fact, the affidavit in support of the order did not mention cell-site simulators at all or seek authorization to conduct any of the sort of electronic surveillance that the Stingrays were apparently performing.

Third, if the government intended this order to cover its use of the two Stingrays, it deliberately misled the state court judge by failing to inform him of the technology being used, the materials to be collected or the nature of the surveillance it was conducting. The affidavit in support of the order fails to mention that the FBI or OPD would be using a Stingray, cell-site simulator or any other similar device. The application does not inform the judge that law enforcement will be using devices wholly independent of the carriers to whom the order was directed. And the affidavit fails to inform the judge that the FBI and OPD would be monitoring *everyone's* phone within range. If the government contends that the order authorized the use of the Stingray, then the agent's statements were necessarily deliberately misleading. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (Kozinski, J., concurring) ("A lack of candor in this or any other aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress seized data). Had the government honestly informed the judge of its intention to use a cell site simulator rather than to obtain records from the carriers, the court undoubtedly would have denied the pen register application. *See In re Application for an order Authorizing Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. 197, 201 (C.D. Cal. 1995) (denying statutory application to use a Stingray because "telephone numbers and calls made by others than the subjects of the investigation could be inadvertently be intercepted").

Fourth, the pen register order was directed only to a single phone number, 510-904-7509, but there is nothing in the application for the order to demonstrate probable cause that that phone number had any relevance to the investigation. The only mention of the phone number in the application is at the end, when the affiant states that he "queried the target number for Ellis" but that statement is not based on any facts demonstrating that the number was in fact Ellis's number and, in fact, the phone was registered to another individual. Boersch Decl. Ex. I at 7 ["Your applicant queried the target

number for Ellis 510-904-7509 . . . . The target number shows to be assigned to Metro PCS and registered to a 'Wendell Stevens' who was a leader of the West Oakland ACORN Gang who [sic] was murdered. Ellis is a member of the [sic] Acorn."]).[10] In short there was nothing to show that the phone number to be "searched" had any connection to the alleged offense.

Fifth, the pen register order certainly does not authorize the use of two Stingrays, and appears to have been obtained (if at all) only in response to a request by OPD.

Finally, the pen register order – which is neither filed nor time-stamped – was apparently signed after the FBI or OPD began using a Stingray so could not have authorized its use by either agency.

3. Even if there had been a Warrant, the Use of the Stingrays Violated the Fourth Amendment as a General Warrant and Lacked Probable Cause

Even if the government had obtained a search warrant for the use of the Stingray, the warrant would be invalid for its lack of particularity because the cell site simulator collected information from and monitored *anyone's* phone that was within range. The Stingray collects information from all phones and sends electronic signals into all homes and devices within its range. Such dragnet surveillance is the sort of general warrant that the Fourth Amendment was explicitly designed to preclude. The purpose of the constitutional requirement of specificity for search warrants is to prevent law enforcement from engaging in general, exploratory searches with no limits on their discretion. *United States v. Cardwell,* 680 F.2d 75, 77 (9th Cir. 1982). Stingrays necessarily collect and monitor all phones within their range, regardless of which particular phone may be "targeted." *See* Lye, *Stingrays.* The government here failed to obtain any judicial authorization for the use of the Stingrays nor was there any safeguard in place to prevent the government from conducting the general, exploratory search the Fourth Amendment is intended to prevent.

C. The Use of the Stingray Likely Violated Title III

If the Stingrays used by OPD and the FBI captured content, or if they could be used as a microphone to eavesdrop on conversations, even if not "capturing" them, as they are capable of

[10] An individual named Wendell Stevenson was alleged to have been a member of a West Oakland gang prior to his murder in 2005. http://www.mercurynews.com/2006/11/30/gang-rivalrykilled-oaklandman-police-say/ (last visited May 1, 2017). The defense is not aware of any alleged Acorn gang member named "Wendell Stevens."

doing, then their use violated Title III. *Patrick*, 842 F.3d at 547 (7th Cir. 2016) (Wood, Chief J., dissenting) ("It seems clear that if the [Stingray] intercepted any cellphone conversations, text messages, or data, Title III covered those interceptions."). It is known that cell-site simulators are "capable of intercepting the contents of communications" and, even more troubling, can convert the target phone into a microphone. *Id.*; Ex. O ("It may be possible [to use a cell site simulator to] to flash the firmware of a cell phone so that you can intercept conversations using a suspect's cell phone as the bug. You don't even have to have possession of the phone to modify it; the 'firmware' is modified wirelessly"). Although the government claims that the Stingrays used in this case did not "capture" or "collect" content, that claim is unsubstantiated and is inconsistent with the evidence produced to the defense. *See, e.g.*, Boersch Decl., Ex. M at REPORTS-DOCUMENTS-000385 and Boersch Decl. ¶19 (PHOTOS-VIDEOS-000035, Disc 3 Track 2 at 4:30) ("Porter, this Omega, I was told there's some activity on the phone right now, because of 108 maybe." "Yeah Omega, he's uh, he's live on his uh every couple minutes."). Those claims also do not address the question whether the Stingrays were simply enabling the FBI and OPD to use Ellis's phone as a microphone.

Under 18 U.S.C. § 2511, any person who "intentionally intercepts . . . any wire, oral, or electronic communication" without following the proper procedures is liable under the statute. 18 U.S.C. § 2511(1)(a). "[E]lectronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). Conversations over cell phones satisfy that definition. *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001) (applying Title III to cell phones, stating "Title III now applies to the interception of conversations over both cellular and cordless phones."). Text messages and cellphone data transmissions also satisfy that definition. *Patrick*, 842 F.3d at 547-48 (Wood, Chief J., dissenting) ("None of the relevant exceptions to that definition [of electronic communication] applies, . . . and there is no reason to think that the interception of text messages or data transmissions would otherwise be excluded from it." (citing *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995) ("The principal purpose of the [Electronic Communications Privacy Act] amendments to Title III was to extend to 'electronic communications' the same protections against unauthorized interceptions that

Title III had been providing for 'oral' and 'wire' communications via common carrier transmissions."); and *Joffe v. Google, Inc.*, 746 F.3d 920, 930 (9th Cir. 2013) (electronic information transmitted over Wi–Fi network does not fit 18 U.S.C. § 2511(g) exceptions). *United States v. Smith*, Case No. 15-20394, 2016 WL 7453761, at *2 (E.D. Mich. Dec. 28, 2016) (if the Stingray "enabled the Government to possibly intercept the contents of conversations and text messages, a Title III order would still be necessary . . . .").

It is undisputed that neither the FBI nor OPD followed the procedures required for an order for electronic surveillance under 18 U.S.C. § 2518. As such, all communications and evidence derived from those communications must be suppressed. *Patrick*, 842 F.3d at 548 (Wood, Chief J., dissenting) ("The remedy for a Title III violation is normally the suppression of the illegally intercepted communications and any evidence derived from them.").

D. Any Evidence Derived from the Illegal Surveillance Must be Suppressed

Evidence derived from an illegal search must be suppressed as the "fruit of the poisonous tree." *Nardone v. United States*, 308 U.S. 338 (1939). Such evidence may include, as it does in this case, the testimony of witnesses. *United States v. Ramirez-Sandoval*, 872 F.2d 1392, 1395-96 (9th Cir. 1989) (testimony of illegal aliens found in van after unlawful search of van suppressed); *United States v. Rubalcava-Montoya*, 597 F.2d 140 (9th Cir. 1979) (testimony of illegal aliens found in trunk of car suppressed as fruits of unlawful search of car). Therefore, any testimony from the people that OPD and/or FBI located and interviewed as a result or because of the information they learned from the illegal use of the Stingray must be suppressed. The discovery produced in the state cases indicates that immediately after or even during the illegal use of the Stingray, the OPD and/or FBI interviewed at least five individuals, whose names were disclosed in the state court proceeding. The government in this case has failed to produce to the defense any witness names or statements; nevertheless, any statements by any witness interviewed as a result of the use of the Stingrays must be suppressed. In addition, any physical evidence that was seized as a result of the illegal use of the Stingrays must also be suppressed.

II. A *FRANKS* HEARING IS REQUIRED BECAUSE THE GOVERNMENT DELIBERATELY MISLED THE COURT IN ITS APPLICATION FOR A PEN REGISTER

If the government contends and this Court concludes that the pen register order somehow authorized the use of the two Stingrays in this case, then it must hold a *Franks* hearing because the government deliberately misled the court about the surveillance it intended to conduct. The government's omission from its application of any information regarding the use or capabilities of the Stingrays violated its duty of candor to the court and prevented the court from exercising its constitutionally mandated role as a neutral reviewer of government action.

A defendant is entitled to a hearing under *Franks* if he makes a substantial preliminary showing that (1) the government "knowingly and intentionally, or with reckless disregard for the truth" made a false or misleading statement to the court; and (2) the affidavit cannot support a finding of probable cause without the allegedly false or misleading information. *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978). The *Franks* rule applies not only to false or misleading statements, but also to deliberate or reckless omissions of material facts. *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985). "Clear proof of deliberate or reckless omission is not required" to show entitlement to an evidentiary hearing. *Id.* All that is required is that the defendant make a substantial showing that the government "intentionally or recklessly omitted facts required to prevent technically true statements . . . from being misleading." *Id.* If, after an evidentiary hearing, the Court finds that the court was misled by false or omitted information, then suppression of the evidence is required. *United States v. DeLeon*, 979 F.2d 761, 763 (9th Cir. 1992).

If the government contends that the order authorized the use of the two Stingrays, its application for the order was seriously deceptive. Nowhere in the application does the affiant – OPD Officer Jason Saunders – refer to or describe a Stingray, cell site simulator, or any equipment similar to the Stingrays actually used. Nowhere in the application does the government reveal that it is not Metro PCS who will be conducting the surveillance but instead that the FBI and OPD will each be using Stingrays to roam around the streets of Oakland monitoring potentially hundreds of individuals' phone calls. Nowhere in the application does the government particularize the information that will be collected from the Stingrays or from whom.

If the government contends that the pen register order and accompanying application were authorization for the Stingrays, there can be no doubt but that the misstatements and omissions in the application were intentional and deliberate. In fact, the government has admitted as much. *See, e.g.*, Lye, *Stingrays*.

CONCLUSION

All evidence derived from the use of the Stingrays should be suppressed. In the alternative, a *Franks* hearing is warranted.

Dated: May 1, 2017

/s/ Martha Boersch
Martha Boersch
Attorney for Defendant
PURVIS LAMAR ELLIS