UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

ELIJAH COOPER,

Defendant.

Case No. 13-cr-00693-SI-1

ORDER DENYING DEFENDANT'S MOTIONS TO SUPPRESS

Re: Dkt. Nos. 72, 73

On February 6 and February 27, 2015, the Court heard argument on defendant's motions to suppress. For the reasons set forth below, the Court **DENIES** defendant's motions.

BACKGROUND

On February 5, 2013, a confidential human source ("CHS"), working with the FBI, engaged in a controlled narcotics purchase with suspect Anthony Knight. Declaration of Ethan A. Balogh ("Balogh Decl.") Ex. B. While the CHS was discussing the terms of the buy with Knight, a white Mercedes pulled into the parking lot and Knight went to meet with the driver of the Mercedes. *Id.* The Mercedes then drove away again. *Id.* Knight then got into the CHS's car, gave the CHS an ounce of crack cocaine, and told the CHS that Knight's supplier had to go back and get the remainder of the drugs. *Id.* When the Mercedes returned to the parking lot, Knight went to meet with the Mercedes's driver again, and then gave the CHS the remainder of the drugs the CHS had paid for. *Id.*

The FBI sought to ascertain who had been driving the white Mercedes. A query to the California Department of Motor Vehicles, based upon the car's license plate number, revealed that the car was registered to a Johnny Ray Trammell. *Id.* Ex. H ¶ 64 n.11. The CHS was shown a

photo of Trammell, but the CHS said that the driver of the Mercedes was younger looking. with close cropped hair. *Id.* ¶ 71. The CHS was then shown a photo of Tony Befford; the CHS identified Befford as the driver. *Id.*

Agents then tried to verify the CHS's identification of the driver as Befford. *Id.* ¶ 72. The agents conducted further surveillance of the white Mercedes, but concluded that the driver was not Befford. *Id.* The agents then asked the San Francisco Police Department ("SFPD") to conduct a traffic stop to determine who the driver was. *Id.* The SFPD complied, and identified the driver as defendant Elijah Cooper. *Id.* Cooper was wearing a royal blue hooded sweatshirt when the SFPD conducted the traffic stop. *Id.*

On February 6, 2013, federal agents asked the CHS about the misidentification of Cooper as Befford. *Id.* ¶ 73. The CHS was then shown a photo of Cooper; the CHS identified Cooper as the driver of the white Mercedes. *Id.* The CHS stated that, during the controlled buy, Cooper's hair was "a bit longer" than depicted in the photo. *Id.* Ex. D. One agent asked the CHS what the driver had been wearing during the controlled drug buy. *Id.* Ex. H. ¶ 73. The CHS responded that the driver of the white Mercedes had been wearing a "royal blue hoodie." *Id.*

On February 21, 2013, the government sought a wiretap for Knight's telephone, and named several individuals, including Cooper, as target subjects for surveillance. *Id.* Ex. G, at 2. On April 4, 2013, the government sought two more wiretaps, one of which was for Cooper's mobile phone. *Id.* Ex. L.

The FBI agents were aware that Cooper, at that time, was serving a term of supervised release for a prior narcotics trafficking conviction. Declaration of Jacob D. Millspaugh ("Millspaugh Decl.") ¶ 2. The agents decided not to contact Cooper directly because they believed that the contact would be noticed and Cooper would be considered a snitch, and thereby placed in danger. *Id.* Therefore, the agents decided to contact Cooper's probation officer, Octavio Magaña, to see if he could help arrange a meeting. *Id.*

On August 16, 2013, FBI agents, SFPD officers, and an Assistant U.S. Attorney ("AUSA") went to Mr. Magaña's office to meet with Cooper. *Id.* ¶ 3. After Cooper arrived and learned who all the individuals were, Cooper was advised that they had evidence he was engaged in drug

dealing, and that it was in his interest to cooperate with them. *Id.* Cooper was not questioned about the crimes under investigation; rather, he was told about some of the evidence against him. *Id.*

On September 26, 2013, following weeks in which Cooper never responded regarding his willingness to cooperate, agents swore out a criminal complaint against Cooper for distribution of cocaine base and conspiracy to distribute. *Id.* ¶ 5. On October 4, 2013, the FBI agents, SFPD officers, and an AUSA, again went to Mr. Magaña's office to meet with Cooper. *Id.* ¶ 6. The AUSA asked Cooper if he had considered what had been discussed at the August, 2013 meeting. *Id.* Cooper stated that he wanted to see a lawyer. *Id.* He was immediately arrested. *Id.*

Two SFPD officers then transported Cooper to the San Francisco Hall of Justice for post-arrest processing. *Id.* ¶ 7. According to Cooper, he was placed in an interrogation room, shown photos of men from his neighborhood, and asked questions about the activities of those men. Declaration of Elijah Cooper ("Cooper Decl.") ¶ 6. Cooper declined to answer any questions. *Id.* Because Cooper was arrested after the Friday morning magistrate calendar had already concluded, Cooper was lodged at the San Francisco County Jail until he could be arraigned on the following Monday. Millspaugh Decl. ¶ 7.

On October 17, 2013, the grand jury returned a two-count indictment against Cooper, charging him with: (1) distribution of cocaine base, in violation of 21 U.S.C. §§ 841 (a)(1), 841 (b)(1)(B)(iii); and (2) conspiracy to distribute cocaine base, in violation of 21 U.S.C. § 846. On July 31, 2014, this Court ruled on eight motions filed by defendant. Docket No. 65. The Court granted defendant's motion to dismiss Count Two of the indictment. *Id.* at 7. On August 28, 2014, the grand jury returned a superseding indictment, charging the same two counts as the original indictment. Docket No. 67.

On November 12, 2014, the Court issued an order dismissing Count Two of the Superseding Indictment, and ordered additional briefing on defendant's motions to suppress, and ordering the government to provide Cooper with certain evidence pertaining to his motions. Docket No. 87. The Court noted in pertinent part:

> The Court finds that it is currently unable to rule on these motions for two reasons. First, there is a significant asymmetry of information between the parties which has heretofore prevented a robust adversarial exchange and meaningful briefing on the defendant's suppression motions. This asymmetry of information stems from the government's refusal to provide Cooper with the applications and orders conferring judicial authorization to obtain pen register, trap and trace, and cell site data. This has led to confusion as to the specific statutory provisions the government relied upon to conduct its various forms of surveillance. Second, the government has simply failed to respond to many of Cooper's substantive arguments.

Id. at 6.

The Court will now proceed to address Cooper's motions to suppress in light of the parties' supplemental briefing.

DISCUSSION

I. Motion to Suppress Evidence Obtained Through Pen Registers and Trap and Trace Devices

Cooper moves to suppress evidence obtained through pen register and trap and trace devices. In an earlier order addressing this issue, the Court noted that the parties presented substantially different accounts premised on highly conflicting information, and that there was some confusion amongst the parties as to what was actually collected through this monitoring process. Docket No. 65 at 25. The Court therefore ordered additional briefing on the issue,[1] specifically requesting that the parties explain (1) what information was collected, (2) how it was collected, and include (3) attached exhibits containing the actual evidence collected. *Id.* In response the government filed a declaration from a Metro PCS employee which describes the information the government collected. The information, which the government terms "pen register data," in the case at bar includes the "incoming call number, outgoing call number, duration of call, call date, time call began, [and] time call ended." Docket No. 66, Thompson Decl. ¶ 3. In addition, the data indicates the geographic coordinates (longitude and latitude) of the cell tower used when the call was initiated, and the tower used at the conclusion of the call ("cell site data").

[1] This would be the first of two rounds of additional briefing ordered by the Court. *See* Docket Nos. 65, 87.

Id. The government was able to obtain this information over a period of 120 days (the 60 days preceding the issuance of the magistrate's order, and 60 days following the issuance of the order).

Cooper argues that this data should be suppressed because (1) the Pen Statute requires a finding of probable cause to obtain prospective cell site data, and (2) the Fourth Amendment requires a showing of probable cause to obtain historical cell site data. The government disagrees, relying on a "hybrid theory" to argue that a lower showing is required.

A. Statutory Framework

(i). The Pen Statute

The Electronic Communications Privacy Act ("ECPA") regulates the means by which government entities may obtain the information of private citizens through electronic surveillance. Title III of the ECPA (the "Pen Statute") governs the use of pen registers and trap and trace devices, and was enacted "to protect effectively the privacy of wire and oral communications." *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001). A trap and trace device is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C.A. § 3127(4). A pen register is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C.A. § 3127(3). Under the Pen Statute, a court *shall* enter an order authorizing the use of a pen register or trap and trace device "if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C.A. § 3123.

In 1994, Congress passed the Communications Assistance of Law Enforcement Act ("CALEA"), which amended certain provisions of the ECPA. In particular, the CALEA prohibits the government from relying solely upon the Pen Statute to obtain cell site data. 47 U.S.C. § 1002(a)(2)(B) ("with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices [...], such call identifying information shall not include any

information that may disclose the physical location of the subscriber."). While the CALEA clearly bars the government from obtaining authorization to obtain cell site data by merely showing that its "use is relevant to an ongoing criminal investigation," it did not explicitly establish a standard for obtaining such data. However, in the absence of congressional intent to the contrary, Federal Rule of Criminal Procedure 41 "provid[es] a default mode of analysis that governs any matter in which the government seeks judicial authorization to engage in certain investigative activities." *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294, 322 (E.D.N.Y. 2005). Under Rule 41, the government must make a showing of "probable cause."

While the question has not been directly addressed by the Ninth Circuit, a number of courts have found that Rule 41 provides the appropriate standard for obtaining prospective, or "real-time," cell site data.[2] *See e.g. United States v. Espudo*, 954 F. Supp. 2d 1029, 1043 (S.D. Cal. 2013) ("Upon review of the statutory scheme, the Court finds that an application for real-time cell site location data does not implicate any statute regulating search or seizure or special circumstances. Accordingly, the terms of Rule 41 govern in the present case."); *cf. In re U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No.*, No. MISC. 06-0186, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006).

(ii). The SCA

Title II of the ECPA, the Stored Communications Act ("SCA"), governs requests for access to stored records, including historical cell site data. Under the SCA, the government may obtain an order to access such records "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to

[2] By providing the location of the nearest cell tower used by the target phone, cell site data is essentially a clumsy version of GPS tracking. This result therefore squares with the statutory framework of the ECPA, which requires a showing of probable cause under Rule 41 for the installation of a tracking device. *See* 18 U.S.C.A. §§ 3104, 3117.

an ongoing criminal investigation."18 U.S.C. § 2703(d).[3]

B. Prospective Cell Site Data

As discussed above, under the CALEA, a showing of probable cause is required to obtain prospective, or real-time, cell site data. However, the government contends that it may rely on the SCA's lower showing of "specific and articulable facts" to obtain real-time cell site data on a prospective basis. The government's position arises from its fundamental disagreement with the binary distinction between prospective versus retrospective cell site data. 12/12/14 Sealed Government Brief at 3 ("whether the records are 'historical' or are captured by the phone company and sent out shortly thereafter or 'prospectively' the showing that the government must make to receive the records is the same – specific and articulable facts.").

The government's position – which has been coined the "hybrid theory" by other courts – is that it may simultaneously rely on provisions of the Pen Statute and the SCA to obtain real time cell site data on the lower showing of "specific and articulable facts." The hybrid theory relies on the wording of the CALEA which prohibits the government from obtaining cell site data "*solely* pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2)(B) (emphasis added). By combining the SCA with the Pen Statute, the Government claims to have complied with the CALEA because it is not *solely* relying on the Pen Statute. Therefore, under the government's hybrid theory, the SCA governs access not only to data which is electronically stored at the time the government seeks access to it, but also to data that is not in existence but that will be recorded and stored at some point in the future.

However, as its name might suggest, the *Stored* Communications Act's "entire focus . . . is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party providers . . . . Nothing in the SCA contemplates a new form of ongoing surveillance." *Espudo*, 954 F. Supp. 2d at 1036. As the

[3] Under 18 U.S.C. § 2703(c)(A), the government may obtain this information by obtaining a warrant under the "probable cause" standard, although it appears that the government relied only on the lower "reasonable grounds" standard under subsection (d).

Espudo court highlighted, the distinctions between the SCA and other provisions of the ECPA put this fact into relief.

> Wiretap orders authorize a maximum surveillance period of 30 days which begins to run no later than 10 days after the order is entered. 18 U.S.C. § 2518(5). Pen/trap orders authorize the installation and use of a pen register for a period "not to exceed sixty days." 18 U.S.C. § 3123(c)(1). By contrast, Congress imposed no duration period whatsoever for § 2703(d) orders. Likewise, Congress expressly provided that both wiretap orders and pen/trap orders may be extended by the court for limited periods of time. 18 U.S.C. §§ 2518(5), 3123(c)(2). There is no similar provision for extending § 2703(d) orders . . . Another notable omission from § 2703(d) is sealing of court records. Wiretap orders and pen/trap orders are automatically sealed, reflecting the need to keep the ongoing surveillance under wraps. 18 U.S.C. §§ 2518(8)(b), 3123(d)(1). The SCA does not mention sealing. Pen/trap orders must also direct that the service providers not disclose the existence of the order to third parties until otherwise ordered by the court. 18 U.S.C. § 3123(d)(2). Section 2705(b) of the SCA authorizes the court to enter a similar non-disclosure order, but only upon a showing of possible adverse consequences, such as "seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(b)(1–5).

Id. at 1036-37.

The cumulative weight of these distinctions shows Congress's intent that the SCA was to be used as a means to obtain data which has already been stored at the time the government seeks to obtain it. While the government relies primary on three cases – from the Southern District of New York and Northern District of Georgia – which lend support to its "hybrid theory," the majority of courts have rejected it as an attempt to circumvent the CALEA's mandate that real time cell site data may be obtained only by a showing of probable cause. *In re Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, No. 06 CRIM. MISC. 01, 2006 WL 468300, at *1 (S.D.N.Y. Feb. 28, 2006) ("join[ing] eight decisions by seven other Magistrate Judges" in rejecting the hybrid theory); *In re U.S. For an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 956 (E.D. Wis. 2006) *aff'd*, No. 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (relying in part on congressional testimony of FBI Director to reject hybrid theory); *In re U.S. for Orders Authorizing Installation & Use of Pen Registers & Caller Identification Devices on Tel. Numbers*, 416 F. Supp. 2d 390, 396 (D. Md. 2006) (the hybrid theory "leaves the court with authority that is at best murky and, at

worst, illusory."); *In re U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No.*, No. MISC. 06-0186, 2006 WL 6217584, at *2 (D.D.C. Aug. 25, 2006) ("Most of the Magistrate Judges that have considered the hybrid theory have found it to be unavailing."); *In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294, 318 (E.D.N.Y. 2005) (disapproving of "the fallacy of the [hybrid theory's] overarching endeavor of stitching together disparate laws to achieve a result that none alone permits."). Accordingly, the Court joins the growing number of district courts which have rejected the hybrid theory's contorted statutory interpretation. A contrary decision would circumvent the very safeguards Congress meant to put in place by enacting the CALEA.

C. Historical Cell Site Data

Cooper also argues that the government must make a showing of probable cause in order to obtain historical cell site data, and that its failure to do so violates his rights under the Fourth Amendment. Conversely, the government argues that it need only comply with the SCA's required showing of "specific and articulable facts." 18 U.S.C. § 2703(d).

The Fourth Amendment protects the right of the people to be secure in their "persons, houses, papers, and effects" against unreasonable searches and seizures. U.S. Const. amend. IV. "A search occurs for Fourth Amendment purposes when the government physically intrudes upon one of these enumerated areas, or invades a protected privacy interest, for the purpose of obtaining information." *Patel v. City of Los Angeles*, 738 F.3d 1058, 1061 (9th Cir. 2013). In order to establish a violation, the defendant must show that he "can claim a justifiable, a reasonable, or a legitimate expectation of privacy that has been invaded by government action." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (internal quotation marks omitted); *see also Crowley v. Holmes*, 107 F.3d 15 (9th Cir. 1997) ("To establish a Fourth Amendment violation, a plaintiff

must show that he had an objectively reasonable expectation of privacy.") (internal citations omitted).

In *Smith v. Maryland*, 442 U.S. 735(1979), the Supreme Court held that the warrantless use of pen registers did not violate the Fourth Amendment, even when a call was placed from within the caller's home. The Court noted that while individuals have a reasonable expectation of privacy in the *content* of their phone conversations, the Fourth Amendment does not extend to information collected by pen registers. However, the pen registers employed in 1979 bear little resemblance to their modern day counterparts. In the early years, "a law enforcement official could not even determine from the use of a pen register whether a communication existed . . . They disclose[d] only the telephone numbers that have been dialed — a means of establishing communication. [They did not capture] any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed [was] disclosed." *Id.* at 741, *citing United States v. New York Tel. Co*., 434 U.S. 159, 167 (1977). Therefore *Smith* does not answer the question of whether persons who place a call have a reasonable expectation of privacy in their location as conveyed by historical cell site data. *Cf. Riley v. California*, 134 S. Ct. 2473, 2488 (2014) (The Supreme Court recently rejected the government's reliance on old cases holding that police could search the physical belongings of an arrestee, in order to justify searching the data on an arrestee's cell phone: "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.").

In *United States v. Jones*, 132 S. Ct. 945 (2012), the Supreme Court held that the installation of a GPS device on the defendant's car, tracking his movements for a month, violated his rights under the Fourth Amendment. The majority opinion, authored by Justice Scalia and joined by three other Justices, held that the installation of the GPS device constituted a warrantless physical trespass onto the defendant's property; as such, the majority found it unnecessary to reach

the question of whether the defendant had a reasonable expectation of privacy in his physical location over the course of a month. Justice Sotomayor concurred with the majority's reasoning, but wrote separately to discuss the potential applicability of individual privacy rights in the digital collection of information indicating their location. Finally, Justice Alito, joined by three other Justices, authored a concurrence which held that Jones did indeed have a reasonable expectation of privacy in the location data conveyed by the GPS device.

In her concurrence, Justice Sotomayor notes that GPS monitoring "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," and that the government's ability to obtain such information without a warrant "may alter the relationship between citizen and government in a way that is inimical to democratic society." *Id.* at 955-56 (Sotomayor, J., concurring) (internal citations omitted). She further questioned the vitality of the idea that individuals have no expectation of privacy in information voluntarily disclosed to third parties, noting that it is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.* at 957. Justice Alito's concurrence went a step further, noting that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy . . . [S]ociety's expectation has been that law enforcement agents and others would not — and indeed, in the main, simply could not — secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.* at 964 (Alito, J., concurring). The Sotomayor and Alito concurrences implicitly adopt the reasoning of the lower court, which held that although Jones' movements were publicly visible, "the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more — sometimes a great deal more — than does the sum of its parts." *United States v. Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010) (emphasis in original). Additionally, even though the majority in *Jones* rested its holding

solely upon the trespassory nature of the installation of the tracking device, it also recognized that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to [the] *Katz* analysis [employed in the concurrences]." *United States v. Jones* 132 S. Ct. at 953 (emphasis in original).

United States v. Davis, 754 F.3d 1205, 1215 (11th Cir.) *vacated pending reh'g en banc*, 573 F. App'x 925 (11th Cir. 2014)[4] is the only case to have considered a suppression motion raising the precise issue of whether warrantless collection of historical cell site data violates a criminal defendant's Fourth Amendment rights.[5] The *Davis* court conducted an exhaustive historical survey of Supreme Court Fourth Amendment jurisprudence, including the recent *Jones* decision. It ultimately held that historical cell site data is within the subscriber's reasonable expectation of privacy. *Id.* at 1218. The court highlighted three primary distinctions between the GPS data (analyzed in *Jones*) and historical cell site data, which militated in favor of finding that a person has a reasonable expectation of privacy in their location as conveyed by historical cell site data. First, it noted that while an automobile is generally confined to traveling on public roadways, a cell phone "can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one." *Id.* at 1216. Second, unlike GPS data, cell site data "is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that

---

[4] Oral argument before the Court *en banc* was scheduled to occur on February 24, 2015 in Atlanta, Georgia. http://www.ca11.uscourts.gov/enbanc-cases

[5] While the Third and Fifth Circuits have addressed the issue, neither was in the context of a suppression motion in a criminal proceeding, and the Third Circuit's decision issued before the Supreme Court decided *Jones*. The Fifth Circuit held that magistrate judges have no discretion to require a showing of probable cause to obtain historical cell site data, and that the "specific and articulable facts" standard was not *per se* unconstitutional. The Third Circuit held that a magistrate judge did indeed have the discretion to require a showing of probable cause. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir.2010); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir.2013).

which would otherwise be private." *Id.* Third, the fact that GPS data may be more precise has no "constitutional significance." *Id.*

While the Ninth Circuit has yet to address this precise question, the Court finds no case which would foreclose adopting the reasoning espoused in *Davis*. In *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), the court held that computer users had no reasonable expectation of privacy in the "to/from" addresses of email messages, or the IP addresses of the websites they visited. However, it noted that its "holding extends only to these particular techniques and does not imply that more intrusive techniques or techniques that reveal more content [*sic*] information are also constitutionally identical." *Id.* at 511. Additionally, in *United States v. Reyes*, 435 F. App'x 596 (9th Cir. 2011), the court declined to address the defendant's argument that the government's collection of his cell site data violated the Fourth Amendment because he failed to raise the issue before the trial court. Nonetheless, the court noted that "[t]he government's use at trial of Reyes's cell site location information raises important and troublesome privacy questions not yet addressed by this court." *Id.* at 598.

Technological advances, coupled with declining cost, have rendered cell phones ubiquitous, and for many, an indispensible gizmo to navigate the social, economic, cultural and professional realms of modern society. *See Jones*, 132 S. Ct. at 963 (there are "more than 322 million wireless devices in use in the United States."). This dynamic dictates that many, if not most, will find their cell phone quite literally attached to their hip throughout the day. *See Riley v. California*, 134 S. Ct. 2473, 2484, 189 L. Ed. 2d 430 (2014) (cell phones are "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."). All the while, these phones connect to cell towers, and thereby transmit enormous amounts of data, detailing the phone-owner's physical location any

time he or she places or receives a call or text.[6] Cell phone users may assume that the numbers they dial will be transmitted to the phone company, thus defeating any reasonable expectation of privacy. However, "there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304, 317-18 (3d Cir. 2010). A cell phone user's reasonable expectation of privacy in his or her location is especially acute when the call is made from a constitutionally protected area, such as inside a home, but is also reasonable even when the call is made in public. *See Davis* 754 F.3d at 127; *cf. Katz* 389 U.S. at 352 ("[Defendant] did not shed his right [to privacy] simply because he made his calls from a place where he might be seen."); *Smith* 442 U.S. at 743 (the "site of the call is immaterial for purposes of [Fourth Amendment] analysis.").

Society's expectation of privacy in historical cell site data is also evidenced by many state statutes and cases which suggest that this information exists within the ambit of an individual's personal and private realm. *See Tracey v. State*, 152 So. 3d 504, 526 (Fla. 2014) (reasonable expectation of privacy in real-time cell site data under US Constitution); *Commonwealth v. Augustine*, 467 Mass. 230, 255 (2014) (under state constitution, defendant had reasonable expectation of privacy in cell site data, requiring government to obtain a warrant before seeking it); *State v. Earls*, 214 N.J. 564, 588 (2013) (same); Colo. Rev. Stat. Ann. § 16-3-303.5(2) (requiring warrant to obtain cell site data); 16 Me. Rev. Stat. § 648 (same); Minn. Stat. Ann. §§ 626A.28(3)(d), 626A.42(2) (same); Mont. Code Ann. § 46-5-110(1)(a) (same); Utah Code Ann. § 77-23c-102(1)(a) (same); *cf. People v. McKunes*, 51 Cal. App. 3d 487, 492 (Ct. App. 1975) (finding a right to privacy in phone records, reasoning that "in this age and place, it is virtually impossible for an individual or a business entity to function in the economic sphere without a

[6] At oral argument on February 6, 2015, the government stated that cell site data is recorded for both calls and text messages.

telephone and that a record of telephone calls also may provide a virtual current biography.") (internal citations omitted). While state law is, of course, not dispositive on this question, "the recognition of a privacy right by numerous states may provide insight into broad societal expectations of privacy." *United States v. Velasquez*, No. CR 08-0730 WHA, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010); *see also Trujillo v. City of Ontario*, 428 F. Supp. 2d 1094, 1106 (C.D. Cal. 2006) *aff'd sub nom. Bernhard v. City of Ontario*, 270 F. App'x 518 (9th Cir. 2008) (the "laws that prohibit or regulate conduct in locker rooms . . . represent society's understanding that a locker room is a private place requiring special protection."); *Maynard*, 615 F.3d at 564 ("state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable.").

The government has many important and appropriate reasons for tracking the cell site data of suspected criminals. Today, the Court only holds that the Fourth Amendment provides the appropriate mechanism to balance the government's interest in law enforcement and the people's right to privacy in their physical location as conveyed by historical cell site data over a period of 60 days.

To be clear, the SCA makes no mention of cell site data, but rather speaks in general terms of "records concerning electronic communication." As a matter of statutory construction, it is axiomatic that "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Const. Trades Council*, 485 U.S. 568, 575 (1988). Accordingly, the Court does not find the SCA to be constitutionally deficient. Rather, the Court assumes, as it must, that Congress could not have intended the SCA to be used to obtain constitutionally protected information absent a showing of probable cause.

D. Good Faith Exception

The government urges that even if the Court finds that probable cause is required to obtain cell site data, the evidence in this case should not be supressed, because of operation of the good faith exception to the exclusionary rule.

In *United States v. Leon*, 468 U.S. 897 (1984), the Supreme Court "held that the exclusionary rule does not apply when the police conduct a search in 'objectively reasonable reliance' on a warrant later held invalid." *Davis v. United States*, 131 S. Ct. 2419, 2428 (2011). "If the purpose of the exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment." *Leon*, 468 U.S. at 919 (citing *United States v. Peltier*, 422 U.S. 531, 542 (1975)). "For exclusion to be appropriate, the deterrence benefits of suppression must outweigh the rule's heavy costs." *Davis*, 131 S. Ct. at 2422 (2011). In general, evidence will not be suppressed when the magistrate, not the officer, errs. *United States v. Mendosa*, 989 F.2d 366, 369 (9th Cir. 1993). Evidence should be suppressed only if: (1) the magistrate has abandoned his detached and neutral role, (2) the officers were dishonest or reckless in preparing their affidavit, or (3) the officers could not have "harbored an objectively reasonable belief that probable cause existed." *Leon*, 468 U.S. at 926.

When presented with the same issue, the Eleventh Circuit found that

> The only differences between *Leon* and the present case are semantic ones. The officers here acted in good faith reliance on an order rather than a warrant, but, as in *Leon*, there was a 'judicial mandate' to the officers to conduct such search and seizure as was contemplated by the court order. As in *Leon*, the officers 'had a sworn duty to carry out' the provisions of the order. Therefore, even if there was a defect in the issuance of the mandate, there is no foundation for the application of the exclusionary rule.

Davis, 754 F.3d at 1218 (internal citations omitted).

The Court concurs with this reasoning. While the magistrate court's order required resolving an unsettled question of law – namely, whether the SCA allows the government to obtain cell site data absent a showing of probable cause – there is nothing in the record to suggest that it "abandoned its detached and neutral role" in arriving at its ultimate conclusion. Contrary to Cooper's suggestions, 1/16/15 Def. Sealed Brf. at 21-22, the Court can find nothing to show that the government was dishonest or misleading in its applications for cell site data. Nor can the Court conclude, given the lack of binding precedent to the contrary, that "a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." *United States v. Luong*, 470 F.3d 898, 902 (9th Cir. 2006) (citing *Leon*, 468 U.S. at 922); *see also Leon*, 468 U.S. at 898 ("Once the warrant issues, there is literally nothing more the policeman can do in seeking to comply with the law, and penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations."). The Court therefore finds that the good faith exception applies, and accordingly, **DENIES** Cooper's motion to suppress pen register and trap and trace data on this basis alone.

II. Motion to Suppress Evidence Obtained Through Wiretap Devices

Cooper argues that the evidence obtained through wiretap devices must be suppressed. First, Cooper points out that government affidavits appear to show that the government commenced electronically surveying him before it obtained the proper judicial authorization. Docket No. 72, Def. Wiretap Mot. at 1-2. Cooper asserts that the information obtained through this unauthorized surveillance contributed to the probable cause showing the government had to make to obtain permission to use wiretaps, and that therefore the wiretap evidence must be suppressed. Second, Cooper highlights that Special Agent May claims in an affidavit that Knight texted Cooper at 2:14pm on February 5, 2013 in order to establish probable cause to obtain a wiretap, yet the records the government has turned over in discovery do not show any text communication between Knight and Cooper during the relevant time period. Finally, Cooper expresses general concerns that the government may be using "Stingray technology and/or the Hemisphere program" in order to conduct unauthorized surveillance. Docket No. 72, Def. Wiretap

Mot. at 3; *see also* Docket No. 74, Balogh Decl.

In the Court's prior order, it directed the government to produce certain documents, and respond in greater detail to Cooper's allegations. Docket No. 87. In response to the Court's order, government's counsel asserts in a sworn declaration that the government did not employ "stingray," "hemisphere," or any other means of surveillance without court order. Tolkoff Decl ¶3. He also explains that that the discrepancy regarding the missing text message was due to Agent May's misclassification of a two-second call as a text message. Tolkoff Decl ¶ 4. In his brief, Cooper attacks the government's explanation as insufficient, primarily because no one with personal knowledge swore to this explanation. 1/16/15 Sealed Def. Brf. at 2. In a reply brief, the government denies surveying Cooper without explicit judicial authorization. 1/30/15 Sealed Gov't Brf. at 3. The government also attached a sworn declaration of Special Agent May, who was the affiant for the wiretap application at issue. Sealed May Decl. ¶ 2. Agent May explains that he erroneously assumed, because of its brevity, that a two second phone contact was a text message, when in fact it was a call, *Id.* at ¶ 4. This would explain the missing text message at 2:14pm on February 5, 2013 of which Mr. Cooper complains. Agent May also declares that neither he, nor anyone else on the investigative team, used unauthorized surveillance techniques. *Id.* at ¶ 6.

The Court is satisfied that the government did not engage in any unauthorized surveillance of Cooper, or thereby rely on tainted evidence in order to establish the probable cause necessary to wiretap Cooper. Accordingly, the Court **DENIES** defendant's motion to suppress evidence obtained through wiretaps.

///

///

CONCLUSION

For the foregoing reasons, the Court **DENIES** Cooper's motions to suppress. This order resolves Docket Nos. 72 and 73.

IT IS SO ORDERED.

Dated: March 2, 2015

SUSAN ILLSTON
United States District Judge