**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA,** | ) | |
| | ) | |
| **v.** | ) | **Criminal Action No. 05-0386 (ESH)** |
| | ) | |
| **ANTOINE JONES, *et al.*,** | ) | |
| | ) | |
| **Defendants.** | ) | |

**MEMORANDUM OPINION AND ORDER**

On January 23, 2012, the Supreme Court vacated Antoine Jones' conviction under 21 U.S.C. § 846 for Conspiracy to Distribute and Possess with Intent to Distribute Five Kilograms or more of Cocaine and Fifty Grams or more of Cocaine Base. *United States v. Jones*, 132 S. Ct. 945 (2012). In that opinion, the Supreme Court unanimously ruled that the government's installation of a GPS device on Jones' car and use of the device to track the car's movement for a period of twenty-eight days constituted a Fourth Amendment search. Relying on that decision, as well as the D.C. Circuit's opinion in this case in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. United States v. Jones*, 132 S. Ct. 945 (2012), defendant now moves to suppress cell-site data covering a four-month period that was obtained pursuant to three orders issued by United States Magistrate Judges of this Court in June, August, and September of 2005. (Defendant's Motion to Suppress Cell Site Data, Mar. 29, 2012 [ECF No. 606] ("Mot.").)

Defendant, with the support of an *amici curiae* brief filed by Electronic Frontier Foundation and Center for Democracy & Technology (Brief Amici Curiae in Support of Defendant Jones' Motion to Suppress, Aug. 13, 2012 [ECF No. 644] ("Amicus Br.")), argues

that under the Fourth Amendment, the government was required to obtain a warrant based on probable cause prior to tracking Jones' location based on cell-site data provided by a third party provider for a four-month period of time. The Court, however, need not resolve this vexing question of Fourth Amendment jurisprudence, since it concludes that the good-faith exception to the exclusionary rule applies.

## BACKGROUND

The facts underlying the indictment in this case have been set forth in detail by this Court, [1] as well as the Circuit Court in *Maynard*, 615 F.3d at 549.[2] Accordingly, the Court will provide a brief summary only of the facts pertinent to the issuance of the three orders granted by the two magistrate judges and a simplified overview of the cellular technology at issue here.

### I. THE ORDERS

As part of their investigation, law enforcement agents sought to obtain cell-site information from Cingular Wireless for two cell phones they believed were being used by defendant. On June 20, 2005, the government filed an Application for Pen Register, Caller Identification Device, Subscriber and Cell Site Information pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d) for cellular telephone number (202) 538-3946. (Mot. ¶ 2.) In that

[1] Jones was first tried with five co-defendants in October 2006 to January 2007. The jury acquitted him of all counts except it hung on the conspiracy count. He was subsequently retried on the one-count conspiracy charge with co-defendant Maynard and after a two-month jury trial, he was convicted on January 10, 2008. In view of Jones' "two or more prior convictions for a felony drug offense," he was sentenced on May 2, 2008, to a mandatory term of life imprisonment as required by 21 U.S.C. § 841(b)(1)(A). The facts underlying the indictments are set forth in this Court's opinions in *United States v. Jones*, 451 F. Supp. 2d 71, 73-74 (D.D.C. 2006), and *United States v. Jones*, 511 F. Supp. 2d 74, 77-78 (D.D.C. 2007).

[2] On appeal, only Jones succeeded in having his conviction vacated by the Circuit Court, and thereafter, on appeal to the Supreme Court, the case was again referred to as *United States v. Jones*.

application, the government included several facts in support of its claim that the cell-site information regarding that phone number would be "relevant and material to an ongoing criminal investigation." First, the government explained that it was believed that the user of cellular telephone number (202) 538-3946 used his phone in furtherance of Title 21, United States Code, Section 841, and was participating in a conspiracy to distribute narcotic controlled substances. (*see* Government's Opposition to Motion to Suppress Cell Site Data, Sept. 4, 2012 [ECF No. 648] ("Opp'n") Ex. A, June 20, 2005 Application ¶ 2.) Second, the government stated that:

> [P]ersons engaged in illegal narcotics trafficking utilize their telephones to arrange meetings at which narcotics are supplied and payment for those narcotics are made. Knowing the location of the trafficker when such telephone calls are made will assist law enforcement in discovering the location of the premises in which the trafficker maintains his supply of narcotics, paraphernalia used in narcotics trafficking such as cutting and packaging materials, and other evidence of illegal narcotics trafficking, including records and financial information. Similarly, knowledge of the location of the trafficker when he places telephone calls to known suppliers and customers can assist law enforcement in this physical surveillance of the subject and in obtaining further relevant evidence of the target's illegal narcotics trafficking activity. The use of a cellular telephone requires that the caller's signal involve the use of cell site in the service provider's system. When the target telephone is a cellular telephone, the location of this cell site and the direction from which the caller's signal was sent provides relevant information to assist law enforcement in the above functions.

(*Id.* ¶ 10.) The government's application was granted by Magistrate Judge Facciola on that same day, and the order authorized the disclosure of the requested material for a period of 60 days. (Mot. ¶ 3.) On August 1, 2005, the government sought an extension of the original order, which was granted by Magistrate Judge Kay for another 60 days. (Mot. ¶ 3.) Finally, on September 19, 2005, the government sought a similar order for cellular telephone number (202) 746-0470, which was granted by Judge Facciola for another 60-day period. (Mot. ¶ 3.) Pursuant to these three orders, four months of data was received from Cingular Wireless for the period June 23, 2005 through October 31, 2005. (Opp'n at 4.)

## II. CELL-SITE LOCATION RECORDS

Cellular telephone companies maintain a system of towers to receive and transmit signals from cell phones. When a cell phone user places or receives a call, the cell phone sends a signal that is picked up by the nearest tower. In the regular course of business, cellular telephone companies generate and retain records of which cell tower a user's phone was connected to at the beginning and end of each call. These records are only generated when the user places or receives a call; no such record is created when the phone is not in use. *See In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) ("Gorenstein Opinion") ("[T]he data is provided only in the event the user happens to make or receive a telephone call.").

Because cell-site data does not identify a user's precise location, but instead only identifies the cell phone tower nearest a user at the time of a call, the precision of cell-site data depends on the distance between cell towers in the user's area. As one court has noted, "towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas." *Id.*[3] Some cell phone towers are further divided into three 120º sectors,

[3] Another court explained the technology behind cell-site data as follows:

> The call-detail information, which is generated only when a cell phone is used, provides the date and time of a call, the number with whom the call occurred, the duration of the call, the direction of the call (whether the call was incoming or outgoing), and the codes for the cell sites and sectors involved in the call. Cell tower records identify the locations corresponding to the codes of the cell towers and sectors appearing in the call-detail information. Typical cell towers have three sectors, but the number can vary from one to several. Each sector services basically a cone extending from the tower out to the limits of the tower's service area. Once the Government obtains the call-detail information and the cell-tower records, the Government plots maps that show the general vicinities in which the

such that the cell phone company can identify which of the three sectors the user was in when the call was placed. However, even that information is generally not precise enough to pinpoint a user's location within a particular building.[4]

Cell-site records may be obtained from the cell phone companies in two ways. The government may obtain this information after the fact, by requesting all such data accumulated over a specified time period. This is known as "historical" cell-site data. Alternatively, the government may seek to obtain this information on a real-time basis going forward from the date of the magistrate judge's order. This is known as "prospective" cell-site data. The information is "identical regardless of whether it is obtained historically or prospectively." (Opp'n at 2.) Each of the government's applications in this case sought prospective cell-site data. In particular, the records obtained over the four-month period show for each call the defendant made or received: "(1) the date and time of the call; (2) the telephone numbers involved; (3) the cell tower to which the customer connected at the beginning and/or end of the call; and (4) the duration of the call." (*Id.*)

---

> cell phone was located during the periods when particular cell-phone calls were made or received. These maps reflect that a call occurred within an area that covers several city blocks. Pinpoint accuracy, or even near-pinpoint accuracy, is not possible with these particular records.

*United States v. Madison*, 2012 WL 3095357, at *4 (S.D. Fla. July 30, 2012).

[4] It may be possible for law enforcement to use signaling information from multiple cell towers to "triangulate" a more precise location for the user placing the call. *See In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 451 n.3 (S.D.N.Y. 2006) ("Kaplan Opinion"). However, the government asserts that it did not obtain such data in this case. (*See* Opp'n at 3.)

## ANALYSIS

Defendant argues that the cell-site data should not be admitted at trial. First, he argues that the government cannot rely upon 18 U.S.C. §§ 2703(c)(1) to justify its obtaining prospective cell-site data from Cingular Wireless because (a) the statute does not permit the disclosure of such data (*see* Defendant's Reply to Government's Opposition, Nov. 26, 2012 [ECF No. 654] ("Reply") at 6-7), and (b) even if it did, the government's application did not make the requisite factual showing to satisfy the statutory standard. (Mot. ¶ 10.). Second, he argues that the government obtained the cell-site data in violation of his Fourth Amendment rights. (*Id.* ¶¶ 8-9.)

### I. THE STORED COMMUNICATIONS ACT

The Stored Communications Act ("SCA") authorizes the government to "require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service" if the government obtains a court order for such information. 18 U.S.C. § 2703(c). Subsection (d) provides that a court order under subsection (c) shall issue only if "the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d).

Defendant, with the support of *amici curiae*, argues that the SCA does not permit the disclosure of prospective cell-site data. (*See* Reply at 6.) Many courts have addressed this question since the applications were granted in this case in June, August, and September 2005. Although courts are divided, a majority of judges (including one of the magistrate judges from this Court who granted two of the applications in *Jones*) have denied the government's requests for such information, holding that prospective cell-site data may only be obtained under Rule 41

upon a showing of probable cause.[5] In contrast, the minority have concluded that the SCA—when read in conjunction with other statutory authority—authorizes the disclosure of prospective cell-site information upon less than probable cause.[6]

---

[5] *See, e.g.*, *In re Application of the United States of America for an Order Relating to Target Phone 2*, 733 F. Supp. 2d 939 (N.D. Ill. 2009); *In re Application of the United States of America for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Authority on a Cellular Telephone*, 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009); *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information*, 497 F. Supp. 2d 301 (D.P.R. 2007) ("McGiverin Opinion"); *In re Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the Number [Sealed]*, 439 F. Supp. 2d 456 (D. Md. 2006); *In re Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification Number (585) 111-1111 and the Disclosure of Subscriber and Activity Information Under 18 U.S.C. § 2703*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information*, 407 F. Supp. 2d 134 (D.D.C. 2006) ("Facciola II Opinion"); *In re Application of the United States of America for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed]*, 416 F. Supp. 2d 390 (D. Md. 2006); *In re Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816 (S.D. Tex. 2006); *In re Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); *In re Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services*, 2006 WL 1876847 (N.D. Ind. July 5, 2006); *In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006); *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747 (S.D. Tex. 2005) ("Smith I Opinion"); *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information*, 407 F. Supp. 2d 132 (D.D.C. 2005) ("Facciola I Opinion"); *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [Sealed] and the Production of Real Time Cell Site Information*, 402 F. Supp. 2d 597 (D. Md.

However, this Court need not weigh in on this debate because even if a defendant could argue that the government did not comply with the SCA, all courts that have addressed the issue have held that the SCA does not provide for a suppression remedy. *See, e.g.*, *United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); *United States v. Hardrick*, 2012 WL 4883666, at *8 n.44 (E.D. La. Oct. 15, 2012) (collecting cases). Section 2708 of the SCA provides that "[t]he remedies and sanctions described in this chapter are the *only* judicial remedies and sanctions for nonconstitutional violations of this chapter." 18 U.S.C. § 2708 (emphasis added). Elsewhere, the Act provides for civil damages, *see id.* § 2707, and criminal penalties, *see id.* § 2701(b), but nowhere does it provide for the suppression of evidence. *See United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act does *not* provide an exclusion remedy.").

This same reasoning also resolves defendant's second statutory claim—that the applications did not contain sufficient "specific and articulable facts" to support the court orders. (*See* Mot. ¶ 10.) Even assuming the applications lacked sufficient factual support, the Court would be powerless to order the suppression of the evidence that the government had obtained.

---

2005); *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005); *In re Applications of the United States of America for Orders Authorizing the Disclosure of Cell Cite Information*, 2005 WL 3658531 (D.D.C. Oct. 26, 2005).

[6] *See, e.g.*, *In re Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information*, 433 F. Supp. 2d 804 (S.D. Tex. 2006); Kaplan Opinion, 460 F. Supp. 2d 448; *In re Application of the United States of America for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F. Supp. 2d 202 (E.D.N.Y. 2008); Gorenstein Opinion, 405 F. Supp. 2d 435; *In re Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 411 F. Supp. 2d 678 (W.D. La. 2006).

*See United States v. Powell*, 444 F. App'x 517, 520 (3d Cir. 2011) (noting that, even if the defendant had demonstrated that the government had failed to provide "specific and articulable facts" under 18 U.S.C. § 2703(d), the SCA "affords no suppression remedy for non-constitutional violations" and so "exclusion would not be the appropriate remedy").

Indeed, in the face of this unanimous view of the limited nature of the remedies under the SCA (*see* Opp'n at 24-26), defendant wisely concedes that suppression is not available. (Reply at 8.) Defendant insists, however, that although § 2708 limits the remedies available for *nonconstitutional* violations of the SCA, his argument is that the government violated his *constitutional* rights under the Fourth Amendment by failing to demonstrate probable cause before obtaining cell-site information under the SCA. (*Id.*) The Court will now turn to that claim.

## II. FOURTH AMENDMENT CLAIM

Defendant and *amici curiae* argue that the government obtained cell-site data in violation of the Fourth Amendment. Specifically, they assert that defendant has a reasonable expectation of privacy in the totality of his movements over time, as reflected by his cell-site data. (Mot. ¶ 8; Amicus Br. at 2-11.) The government responds that cell-site information is not sufficiently accurate to allow the government to track the defendant into constitutionally protected spaces—such as the home—or to provide a detailed and holistic picture of the defendant's movements. (*See* Opp'n at 13-19.) The government further insists that there is no reasonable expectation of privacy in the business records of a third party—the cell phone company—particularly when those records are voluntarily turned over to the cell phone company by using one's cell phone. (*See id.* at 5-12.) In the alternative, the government argues that the exclusionary rule should not

apply because the law enforcement officers relied in good faith on the text of 18 U.S.C. § 2703, on magistrate judges' orders and on binding appellate precedent. (*See id.* at 19-22.)

### A. Governing Standard

The Fourth Amendment guarantees that "[t]he 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." U.S. CONST. amend. IV. The Supreme Court has determined that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). More recently, the Supreme Court in this case has held that "the Government's installation of a GPS device on [Jones'] vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" *Jones*, 132 S. Ct. at 949. The majority's holding was premised on the fact that the government had physically intruded onto defendant's private property for the purpose of obtaining information. *See id.* at 949-54.[7] The Supreme Court made clear that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953; *accord id.* at 955 (Sotomayor, J., concurring). Here, there was no comparable trespass on Jones' physical

[7] While the Court was unanimous in affirming the result in *Maynard*, the majority opinion, authored by Justice Scalia, concluded that the physical act of installing a GPS device on the defendant's vehicle was a trespass and a Fourth Amendment search. *Jones*, 132 S. Ct. at 949 ("The government physically occupied private property for the purpose of obtaining information."). The majority was joined by Chief Justice Roberts and Justices Kennedy, Thomas and Sotomayor. The Court expressly declined to consider whether such a "search" violated an individual's reasonable expectation of privacy. *Id.* at 950.

property; instead, there was the mere "transmission of electronic signals."[8] Thus, the traditional reasonable-expectation-of-privacy test applies.

The constitutionality of allowing law enforcement to obtain cell-site data absent a warrant supported by probable cause has been vigorously debated in recent jurisprudence. With respect to *historical* cell-site data, numerous courts have addressed this question, and a majority have concluded that there is no reasonable expectation of privacy in such data.[9] Most of these cases

---

[8] Since *Jones* was decided, all cases that have considered its applicability to cell-site data have concluded it to be irrelevant. *See, e.g.*, *In re application of the United States of America for an Order Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Information and Cell Site Information*, 849 F. Supp. 2d 177, 178 (D.Mass. 2012) ("Collings Opinion") (finding *Jones* inapplicable to the issue of obtaining cell-site data because "the Court Order allowing the government to obtain the records does not involve any attachment of any device on any of an individual's real or personal property"); *United States v. Graham*, 846 F. Supp. 2d 384, 396 (D. Md. 2012) (finding *Jones* inapplicable to the issue of obtaining cell-site data because it "does not involve a physical trespass to property"); *Garcia v. Bradt*, 2012 WL 3027780, at *5 (S.D.N.Y. July 23, 2012) (denying habeas petition seeking retroactive application of *Jones* in part because the alleged tracking of defendant's movements through cell phone records involved "no such physical occupation of petitioner's property"); *United States v. Gordon*, No. 09-153-02 (D.D.C. Feb. 6, 2012) ("Urbina Opinion") (rejecting proposition that *Jones* requires suppression of cell-site location information).

[9] For cases holding that there is no reasonable expectation of privacy in historical cell-site records, *see, e.g.*, *United States v. Madison*, 2012 WL 3095357, at *9 (S.D. Fla. July 30, 2012); *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012); Urbina Opinion, No. 09-153-02; *In re Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [Sealed]*, No. 11-449 (D.D.C. Oct. 3, 2011) (vacating Magistrate Judge Facciola's Aug. 17, 2011 order) ("Lamberth Opinion"); *United States v. Dye*, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011); *United States v. Benford*, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010); *United States v. Jenious*, No. 09-97 (E.D. Wis. Aug. 28, 2009) (Magistrate Judge Gorence's recommendation); *United States v. Suarez-Blanca*, 2008 WL 4200156, at *8-11 (N.D. Ga. Apr. 21, 2008); *In re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F. Supp. 2d 76, 80-81 (D. Mass. 2007) ("Stearns Opinion"). For cases reaching the opposite conclusion, *see, e.g.*, *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010); *In re Application of the United States of America for Historical Cell Site Data*, 747 F. Supp. 2d 827 (S.D. Tex. 2010) ("Smith II Opinion"), *appeal docketed*, No. 11-20884 (5th Cir. Dec. 14, 2011) (oral argument held on Oct. 2, 2012); *In re Application of the United State of America for an Order Authorizing*

have relied on the "third-party doctrine," established in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), which provides that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-44; *see also Miller*, 425 U.S. at 442-44. In *Miller*, the Supreme Court found that a bank customer had no reasonable expectation of privacy in financial information that he voluntarily conveyed to the bank for it to use in the ordinary course of business. 425 U.S. at 442. And in *Smith*, the Court similarly held that the defendant did not have a reasonable expectation of privacy in the numbers he had dialed from his telephone, because he voluntarily conveyed that information to his cellular telephone company when he placed the calls. 442 U.S. at 742-45.

Applying the third-party doctrine, most federal judges—including two from this Court—have concluded that defendants have no reasonable expectation of privacy in historical cell-site data because (a) they voluntarily conveyed their location information to the cell phone company when they initiated a call and transmitted their signal to a nearby cell tower, and (b) the companies maintained that information in the ordinary course of business. *See, e.g.*, *Graham*, 846 F. Supp. 2d at 397-401; *Madison*, 2012 WL 3095357, at *7-9; Urbina Opinion, No. 09-153-02, at 2-3; Lamberth Opinion, No. 11-449, at 9-11; *Benford*, 2010 WL 1266507, at *2-3; *Suarez-Blanca*, 2008 WL 4200156, at *8-9; *but see, e.g.*, Smith II Opinion, 747 F. Supp. 2d at 843-45 (rejecting third-party doctrine because most individuals do not know that use of their cell phone

---

*the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) ("Garaufis Opinion").

All of the cases that have found a reasonable expectation of privacy in historical cell-site data have done so in the context of a government application for an order under the SCA, not in response to a motion to suppress such data after it was obtained.

creates a record of their location and therefore do not "voluntarily" convey that information to the third-party cell phone company).[10]

Other courts, at least prior to *Jones*, have analyzed cell-site location information under the Supreme Court's "tracking devices" cases. In *United States v. Knotts*, 460 U.S. 276 (1983), the Supreme Court held that the use of a tracking device to follow movements on public highways did not implicate Fourth Amendment concerns, because the defendants had no reasonable expectation of privacy while in plain view on public thoroughfares. *Id.* at 282-84. In *United States v. Karo*, 468 U.S. 705 (1984), by contrast, the Court held that the use of a tracking device to determine the specific location of the tracked material within a private residence was a Fourth Amendment search because that fact "could not have been visually verified." *Id.* at 715. Because cell-site data is typically not precise enough to identify the particular building from which a suspect placed a phone call, several courts, relying on the *Knotts/Karo* distinction, have found that such information does not constitute a Fourth Amendment search. *See, e.g.*, *In re Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304, 312-13 (3d Cir. 2010); *Suarez-Blanca*, 2008 WL 4200156, at *9-11; Kaplan Opinion, 460 F. Supp. 2d at 462 (noting that if such information could track an individual into a private home then it might raise Fourth Amendment concerns).

Among the courts that have come to the opposite conclusion that the use of cell-site data obtained without a warrant based on probable cause constitutes a Fourth Amendment search, many have relied on the D.C. Circuit's opinion in *Maynard*. There, this Circuit applied the "mosaic theory," under which law enforcement activities which, standing alone, do not violate

[10] As noted, this case has been argued in the Fifth Circuit and is still pending. *See supra* note 9.

the Fourth Amendment, may nevertheless do so when viewed in the aggregate. *Id.* at 562-64. Thus, even though the government could have physically followed Jones's car in public spaces without violating the Fourth Amendment, the government's use of a GPS tracking device to record his movements over a month-long period violated his reasonable expectation of privacy in the *totality* of his movements. *Id.* at 563.[11] This approach also appears to enjoy support among the concurring justices in *Jones*. For instance, Justice Alito—in a concurrence joined by Justices Ginsburg, Breyer, and Kagan—noted that although "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (internal citation omitted). Similarly, Justice Sotomayor pondered whether there is a "reasonable societal expectation of privacy in the sum of one's public movements." *Id.* at 956 (Sotomayor, J., concurring). However, as correctly agued by the government (*see* Opp'n at 16-17), the rationale adopted in *Maynard* was not endorsed by the majority opinion in *Jones*.[12] In response

[11] Prior to the Supreme Court's decision in *Jones*, several courts applied this analysis to historical cell-site data and determined that the constitutionality of law enforcement's actions turned on the duration of the period of surveillance in question. *See, e.g.*, Smith II Opinion, 747 F. Supp. 2d at 838-40 (finding government request for cell-site records covering 60-day period constituted a Fourth Amendment search under *Maynard* mosaic theory); Garaufis Opinion, 809 F. Supp. 2d at 126 (finding that *Maynard* mosaic theory constitutes an exception to third-party doctrine where government sought cell-site records for 113-day period); *In re Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 2011 WL 679925, at *2 (E.D.N.Y. Feb. 16, 2011) ("Orenstein Opinion") (authorizing government to obtain cell-site data for three windows of time—3 days, 6 days, and 12 days—because such data would not "be as revealing as the sustained month-long monitoring at issue in *Maynard*"); Lamberth Opinion, No. 11-449 at 10-11 (authorizing government to obtain cell-site data because, unlike the prolonged surveillance of a person's movements with GPS tracking that occurred in *Maynard*, the application in that case requested historical cell-site data for "limited numbers of specific calls").

to Justice Alito's suggestion of a distinction between short-term tracking and longer-term monitoring, Justice Scalia, writing for the majority, dismissed it as "a novelty" whose basis "remains unexplained." *Id.* at 954.[13] (*See also supra* note 8.)

As this discussion reveals, there is a robust debate over the question of whether the Fourth Amendment applies to cell-site data obtained from a cellular provider, but to date, this Court knows of no federal court that has held that the use of *prospective* cell-site records constitutes a search under the Fourth Amendment, or of any federal court that has suppressed any type of cell-site data obtained pursuant to a court order under the SCA.[14] While this issue may someday receive the attention of the Supreme Court,[15] this Court need not decide whether the

---

[12] As noted by Justice Scalia, although electronic surveillance without physical trespass "may be . . . an unconstitutional invasion of privacy, . . . the present case does not require us to answer that question." *Jones*, 132 S. Ct. at 954.

[13] Lower courts have refused to apply either the mosaic theory endorsed by the D.C. Circuit or the distinction suggested by the concurrence in *Jones* to cell-site data. *See, e.g.*, Urbina Opinion, No. 09-153-02 at 2; *Graham*, 846 F. Supp. 2d at 404-05, Collings Opinion, 849 F. Supp. 2d at 178-79.

[14] To be sure, many courts have concluded that the government can only obtain prospective cell-site information upon a showing of probable cause. (*See supra* note 5.) However, those courts found that there was no statutory authority under which a court could authorize the disclosure of such information upon a showing of less than probable cause. *See, e.g.*, Smith I Opinion, 396 F. Supp. 2d 747; Facciola I Opinion, 407 F. Supp. 2d 134. They did not make an independent determination that the use of such information violates an individual's reasonable expectation of privacy and therefore constitutes a violation of the Fourth Amendment. *See, e.g.*, McGiverin Opinion, 497 F. Supp. 2d at 311-12 ("[T]he decision in this was arrived at as a matter of statutory construction and likely is not constitutionally required. . . . Thus, Congress could authorize disclosure of limited cell site information on a showing of less than probable cause if it decided to do so. What is clear to me, however, is that Congress has not authorized disclosure of cell site information in the statutes proffered by the government—namely the Pen Register Statute combined with the SCA.").

[15] As observed by Justice Sotomayor in her concurrence in *Jones*, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." 132 S. Ct. at 957.

government violated the Fourth Amendment when it obtained the cell data from Cingular Wireless, since the well-recognized good-faith exception bars the application of the exclusionary rule to this case. *See Ferguson*, 508 F. Supp. 2d at 9-10 (declining to consider the constitutionality of the SCA because the government's reliance on it was objectively reasonable); *Hardrick*, 2012 WL 4883666, at *5 ("the good-faith exception applies and is dispositive"; "[b]y declining to reach this Fourth Amendment issue the Court is applying the 'sound judicial practice of refusing to decide or address issues whose resolution is not necessary to dispose of a case, unless there are compelling reasons to do otherwise'"); *Graham*, 846 F. Supp. 2d at 405-06. Therefore, the Court will decline defendant's invitation (*see* Reply at 5) to decide whether a constitutional violation occurred in 2005 in this case. *See United States v. Webb*, 255 F.3d 890, 904 (D.C. Cir. 2001) (holding that good-faith exception applied and suppression was not appropriate despite the fact that "the question remain[ed]" whether the warrant was supported by probable cause).

**B. Good-Faith Exception**

Ordinarily, the appropriate remedy for a Fourth Amendment violation is suppression of the illegally-obtained evidence. *See Mapp v. Ohio*, 367 U.S. 643 (1961). The purpose of the exclusionary rule is not to remedy a violation of an individual's rights, but rather to deter future unlawful police conduct. *Illinois v. Krull*, 480 U.S. 340, 346 (1987). With that purpose in mind, the Supreme Court has made clear that exclusion is not required "when the police act with an objectively reasonable good-faith belief that their conduct is lawful." *Davis v. United States*, 131 S. Ct. 2419, 2427 (2011) (internal quotation marks omitted). In such cases, "the magnitude of the benefit conferred on such guilty defendants [by the exclusionary rule] offends basic concepts of the criminal justice system," *United States v. Leon*, 468 U.S. 897, 907-08 (1984), and so

suppression is not warranted. The Supreme Court has held that the good-faith exception applies in the following situations: (1) where law enforcement officers reasonably relied on a search warrant issued by a neutral magistrate, despite the fact that the warrant was later found to be defective, *Leon*, 468 U.S. at 920-21; (2) where law enforcement officers reasonably relied on a statute that was later determined to be unconstitutional, *Krull*, 480 U.S. at 349-50; and (3) where law enforcement officers reasonably relied on binding appellate precedent that was later overruled. *Davis*, 131 S. Ct. at 2429. Under at least two of these situations, it is clear that the government can rely on the good-faith exception.[16]

First, it was reasonable for the officers to apply for cell-site data under 18 U.S.C. § 2703. That section states that the government may obtain "record[s] or other information" relating to a cellular telephone company's subscribers. *See* 18 U.S.C. § 2703(c). Numerous courts have held that § 2703(c) permits the government to obtain *historical* cell-site data. *See, e.g.*, Orenstein Opinion, 2011 WL 679925; *Graham*, 846 F. Supp. 2d at 396; *Suarez-Blanca*, 2008 WL 4200156; Stearns Opinion, 509 F. Supp. 2d at 79-80. Although a majority of courts have determined that § 2703(c) does *not* also permit the government to obtain *prospective* cell site data, some courts have reached an opposite conclusion. (*See supra* note 5.) In addition to a situation where reasonable minds may differ as to whether § 2703 permits law enforcement to seek authorization for prospective cell-site information, as far as this Court is aware, no case had addressed the applicability of § 2703(c) to cell-site data—historical or prospective—at the time the government applied for orders in this case on June 20, 2005. Thus, at that time "[i]t was

[16] The rule in *Davis* only applies if there is binding appellate precedent on point. 131 S. Ct. at 2429. Given the Court's analysis under *Leon* and *Krull*, it need not decide if *Smith v. Maryland* was sufficiently on point to be considered binding. *But see, e.g.*, Urbina Opinion, No. 09-153-02 at 2-3 (finding that third-party doctrine of *Smith* applies to cell-site records).

unclear whether a warrant was required, and it was therefore objectively reasonable for law enforcement to request the Orders." *Hardrick*, 2012 WL 4883666, at *7.

Indeed, the Supreme Court itself explained in *Leon* that evidence should only be suppressed "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." 468 U.S. at 919 (citation omitted). Because the state of the law was completely uncharted, the officers here cannot be charged with knowledge that § 2703(c) does not apply to prospective cell-site data, especially given the fact that even now, seven years later, there is still no definite resolution of this question by any appellate court. *See also United States v. Skinner*, 972 F.2d 171, 176 (7th Cir. 1992) (holding that officers had acted in good faith because at the time of their actions the question of what amount of corroboration was required for an anonymous tipster's factual assertions was unsettled).

Because at the time of the applications in this case it was reasonable for the officers to seek an order authorizing the disclosure of cell-site data, it was also reasonable for them to rely on the magistrate judges' orders granting those applications. "[T]he Supreme Court has flexibly applied the good-faith exception embraced in *Leon* to situations beyond law enforcement's reliance on a defective warrant issue by a neutral magistrate." *Hardrick*, 2012 WL 4883666, at *5 (collecting cases). Several federal courts have recently extended *Leon* to exactly this situation—where law enforcement reasonably relied on a court order under 18 U.S.C. § 2703(d). *See id.* at *7; *Suarez-Blanca*, 2008 WL 4200156, at *11-13; *Graham*, 846 F. Supp. 2d at 406. This Court agrees with the rationale of these cases that the underlying goals of the exclusionary rule would not be furthered by suppressing evidence where officers reasonably relied on such judicial orders.

Here, Magistrate Judge Facciola—and later Magistrate Judge Kay—considered the government's applications and determined that the government could obtain prospective cell-site information under 18 U.S.C. § 2703(c) and had satisfied the standard set forth in § 2703(d). "A magistrate is not 'inclined to ignore or subvert the Fourth Amendment,' and law enforcement is 'not expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient.'" *Hardrick*, 2012 WL 4883666, at *7 (citing *Leon*, 468 U.S. at 916, 921). Thus, it was objectively reasonable for the government to rely on the independent judicial determinations that no warrant was required. Moreover, "[t]he fact that [two] neutral Magistrate Judge[s] approved the Government's applications under the SCA provides further reason to deem the Government's reliance on the SCA to be objectively reasonable." *Ferguson*, 508 F. Supp. 2d at 9; *see also United States v. Rowland*, 145 F.3d 1194, 1207 (10th Cir. 1998) ("[A]t the time the warrant was issued and executed, this circuit had not yet ruled on the constitutionality of anticipatory warrants and had not set out conditions on the validity of such warrants. Given the unsettled state of the law, it was not unreasonable for the officers to rely on the magistrate's authorization."). Thus, suppression is not the appropriate remedy for any constitutional violation that may have occurred.

The defense's only argument for why the good-faith exception should not apply is that Magistrate Judge Facciola was acting "merely as a rubber stamp for law enforcement" when he granted the applications. (Reply at 7 (citing *Leon*, 468 U.S. at 914).) This proposition has no basis in fact except for defendant's observation that after Judge Facciola granted the applications in the instant case, he changed his position and began denying similar requests. *See, e.g.*, Facciola I Opinion, 407 F. Supp. 2d 132; Facciola II Opinion, 407 F. Supp. 2d 134. However, the Court is not persuaded that merely because a judge reconsiders an issue at a later date and

arrives at a different conclusion, he must have been acting as a "rubber stamp" in the first instance. There is no evidence in the record to support such a frivolous contention with respect to Judge Facciola, and in fact, quite to the contrary, his willingness to closely consider the legal ramifications of an application for cell-site data in December 2005 despite having granted several similar applications within the previous six months demonstrates the seriousness with which Judge Facciola approached his job.

The Supreme Court has "repeatedly rejected efforts to expand the focus of the exclusionary rule beyond deterrence of culpable police conduct." *Davis*, 131 S. Ct. at 2432. Here, the actions of law enforcement officials were objectively reasonable when they acquired prospective cell data under the SCA from a third-party provider. Given the unsettled nature of the law in 2005, which has remained the case even up to the present, it was reasonable for them to believe that the Fourth Amendment was not implicated. It was also reasonable for them to rely on the three orders of the magistrate judges that granted them the access to the information they now seek to admit at trial. There can therefore be no finding of police culpability, *id.* at 2428, and the good-faith exception will be applied.

**CONCLUSION**

For the foregoing reasons, defendant's Motion to Suppress Cell-Site data is **DENIED**.

/s/
ELLEN SEGAL HUVELLE
United States District Judge

Date: December 14, 2012