

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

UNITED STATES OF AMERICA	:	
	:	
v.	:	Case No. 05-CR-386(1) (ESH)
	:	
ANTOINE JONES,	:	
Defendant.	:	

OPPOSITION TO MOTION TO SUPPRESS CELL SITE DATA

The United States of America, by its attorney, the United States Attorney for the District of Columbia, respectfully opposes defendant’s Motion to Suppress Cell Site Data (document #606; referred to herein as “Deft. Mem.”) and the brief filed by amicus Electronic Frontier Foundation (document #644). For the reasons set forth below, and any other arguments which may be made at a hearing on this matter, the Government submits that the motion should be denied.

Defendant seeks suppression of cell-site location records for his cellular phone – obtained pursuant to orders granted by two Magistrate Judges of this Court – on two grounds. First, defendant argues that the third-party records at issue enjoy protection under the Fourth Amendment and can only be obtained with a search warrant based on probable cause. In the alternative, defendant claims that the government’s applications failed to make the necessary factual showing and that he is therefore entitled to statutory suppression.

On the first point, governing precedent is clear that this data, provided to a third party as an inherent part of the operation of the phone, lacks Fourth Amendment protection. In any event, the officers relied on facially valid judicial and statutory authorization, and suppression is therefore not an available remedy. As to the second claim, the orders met the statutory standard, and, even if they did not, the statute involved provides no suppression remedy.

FACTUAL BACKGROUND

A. Overview of cellular technology and cell-site record creation and retention

In the regular course of their business, cellular telephone companies generate and retain records of certain information associated with their customers' calls. The records at issue in this case 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. The records may also, but do not always, specify a particular sector of a cell tower used to transmit a call.¹ These records may be obtained from the carrier after the fact or, as in this case, contemporaneously with the call event; the information is identical regardless of whether it is obtained historically or prospectively. No such record is created when the phone is not in use.

Although cell tower records provide limited information, that information is useful to law enforcement because it provides a general indication of where a cell phone call was made. As one court has explained,

[t]he information does not provide a "virtual map" of the user's location. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These 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.

In re Application, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (*Gorenstein Opinion*) (citation

¹ Cell towers are often divided into three 120° sectors, with separate antennas for each of the three sectors. To the extent this information does exist in a particular instance, it does not provide precise information regarding the location of the cell phone at the time of the call, but instead only identifies which of the three 120°, pie-slice sectors where the phone was probably located.

omitted).² Only two months ago, another district court reaffirmed these essential facts about cell-site location records:

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 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).

Critically, no Global Positioning System ("GPS") data or other more precise location information (such as "triangulation" data) is contained in the records obtained by the government in this case.³

B. The applications and orders

On June 20, 2005, August 1, 2005, and September 19, Magistrate Judges John Facciola and Alan Kay of this Court entered orders pursuant to 18 U.S.C. §§ 3122 *et seq.* and 2703 authorizing the United States to obtain from a wireless service provider several kinds of information about a cell phone utilized by the defendant. (Copies of the Applications and Orders are attached as Exhibit A.)

² In order to reduce confusion, citations in this memorandum to district court opinions involving government applications under § 2703(d) (typically captioned "In re Application ...", etc.) identify the case by the name of the authoring judge.

³ No "pinging" of the cellular phone to obtain geolocation data occurred here, as amici curiae suggests. *See* brief Amici Curiae 5-6.

Among the data to be provided was the cell site/sector associated with each call placed to or from the target telephone used by defendant. In support of its requests for these orders, the United States stated that “[b]ased upon reliable information, it is believed that the user(s) of cellular telephone (202) 538-3946, subscribed to by Denise Jones ..., utilizes the cellular telephone in furtherance of Title 21, United States Code, Section 841 and is a participant in a conspiracy to distribute and to possess with intent to distribute narcotic controlled substances.” Applications ¶ 2. The Applications further averred that this information would “provide the agents with investigative leads and potential evidence at trial concerning contacts made by the targets in the course of their criminal activity.” *Id.* ¶ 3. As to cell-site records in particular, the applications pointed out that knowing the location of a drug trafficker at the time of various call events is of significant investigative value, *inter alia*, in locating facilities used to store, package, and process narcotics and in conducting physical surveillance. *Id.* ¶ 10. Pursuant to the Orders, four months of data was obtained (from June 23, 2005 through October 31, 2005), not six months as amici curiae allege.

SUMMARY OF ARGUMENT

Defendant’s motion to suppress cell-site location records cannot succeed under any theory. To begin with, no reasonable expectation of privacy exists in the routine business records obtained from the wireless carrier in this case, both because they are third-party records and because in any event the cell-site location information obtained here is too imprecise to place a wireless phone inside a constitutionally protected space. Even if defendant were able to establish a Fourth Amendment privacy interest, the government’s good-faith reliance upon judicial and statutory authorization here forecloses any claim for suppression.

Finally, defendant expressly admits that the government lawfully relied upon the proper legal authority – 18 U.S.C. § 2703(d) – to obtain the disputed records. To the extent that defendant alleges that the government violated this (or other) statutes, his motion fails because no statutory suppression remedy is available. As a result, defendant’s motion must be denied.

ARGUMENT

A. Defendant is not entitled to suppression under the Fourth Amendment

Initially, defendant suggests that he had a reasonable expectation of privacy in cell-site location information routinely conveyed to (and retained by) his wireless telephone company, and that his Fourth Amendment rights were violated when the government obtained those records from the carrier. This conclusion is incorrect for multiple reasons. First, under the established principles of *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), there is no reasonable expectation of privacy in such information, and, accordingly, no Fourth Amendment-protected privacy interest. Second, cell-site information is far too imprecise by any measure to intrude upon a reasonable expectation of privacy. Thus, defendant’s claim of entitlement to constitutional suppression fails.

1. A subscriber has no expectation of privacy in cell-site records generated and retained as routine business records by a third party

The cell-site data that the government obtained via court order in this investigation was not in the hands of the cell phone user at all, but rather in the business records of a third party – the cell phone company. The Supreme Court has held that a customer has no privacy interest in business records of this kind. Addressing a Fourth Amendment challenge to a third party subpoena for bank

records, the Court held in *United States v. Miller*, 425 U.S. 435 (1976), that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440; see also *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party ... he cannot object if the third party conveys that information or records thereof to law enforcement authorities"). Thus, an individual has no Fourth Amendment-protected privacy interest in business records, such as cell-site usage information, that are kept, maintained and used by a cell phone company in the normal course of business. If anything, the privacy interest in cell-site information is even less than the privacy interest in a dialed phone number or bank records. The location and identity of the cell phone tower handling a customer's call is generated internally by the phone company and is not, therefore, typically known by the customer. A customer's Fourth Amendment rights are not violated when the phone company reveals to the government its own records that were never in the possession of the customer.

Further, even if it were the case that cell-site information is disclosed by the subscriber to the telephone company, the Supreme Court's reasoning in *Smith v. Maryland* leads to the same result. In *Smith*, the Court held both that telephone users have no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. See *Smith*, 442 U.S. at 742-44. The Court's reasoning applies equally to cell-site information. First, the Court stated: "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. Similarly, cell phone users understand that they

must send a radio signal, which is received by a cell phone company's antenna in order to route their call to its intended recipient. (Indeed, cell phone users are intimately familiar with the relationship between call quality and radio signal strength, as typically indicated by a series of bars on their phones' displays.)⁴

Second, under the reasoning of *Smith*, any subjective expectation of privacy in cell-site information is unreasonable. In *Smith*, the Court explicitly held that “even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable.” *Id.* at 743 (internal quotation omitted). It noted that “[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44. In *Smith*, the user “voluntarily conveyed numerical information to the telephone company” and thereby “assumed the risk that the company would reveal to the police the numbers he dialed.” *Id.* at 744.

The D.C. Circuit has rejected a Fourth Amendment challenge from journalists to subpoenas directed to their telephone records. *See Reporters Committee for Freedom of the Press v. AT&T*, 593 F.2d 1030, 1042-46 (D.C. Cir. 1978). The court explained that when an individual transacts business with others, “he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair.” *Id.* at 1043. Regarding telephone records in particular, the court held that “[t]he expectation of privacy attaching to telephone conversations relates to the content of the conversations themselves and not to the fact that a conversation took place. No one justifiably could expect that the fact that a particular call was

⁴ “Can you hear me now?” was the familiar jingle from Verizon Wireless commercials and advertisements, making the case to local consumers that Verizon offered a wider range of coverage than other regional service providers.

placed will remain his private affair when business records necessarily must contain this information.” *Id.* at 1045-46. The court rejected the journalists’ Fourth Amendment claims based on “the well-settled rule that a person has no expectation of privacy in the business records of a third party and, therefore, has no interest protected by the Fourth Amendment in such records.” *Id.* at 1043-44.

Because cell-site records are the business records of the phone company pertaining to a transaction with a customer, *Reporters Committee* demonstrates that a customer has no reasonable expectation of privacy in those records. When a cell phone user transmits a signal to a cell tower for his call to be connected, he thereby assumes the risk that the cell phone provider will create its own internal record of which of the company’s towers handles the call. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no expectation of privacy in cell-site information.

For these reasons, **no federal court has ever suppressed cell-site location records**. On the contrary, numerous courts have applied these longstanding constitutional principles to deny similar suppression motions. *See United States v. Madison*, 2012 WL 3095357 at *7-*9 (S.D. Fla. July 30, 2012); *United States v. Dye*, 2011 WL 1595255 at *9 (N.D. Ohio Apr. 27, 2011); *United States v. Velasquez*, 2010 WL 4286276 at *5 (N.D. Cal. Oct. 22, 2010); *United States v. Benford*, 2010 WL 1266507 at *3 (N.D. Ind. Mar. 26, 2010); *United States v. Jenious*, No. 09-Cr-097 (E.D. Wis. Aug. 28, 2009) (unpublished) (copy attached as Exhibit B), *United States v. Suarez-Blanca*, 2008 WL 4200156 at *23 (N.D. Ga. Mar. 26, 2008); *Mitchell v. State*, 25 So. 3d 632 (Fla. Dist. Ct. App. 2009).

Two recent federal decisions from the Washington, D.C. area underscore the lack of any valid Fourth Amendment privacy interest in cell-site location records. In *United States v. Graham*, 2012

WL 691531 (D. Md. Mar. 1, 2012), the Government had obtained cell-site location records for the defendants' phones covering various periods coinciding with a series of armed robberies. The defendants claimed that the Government improperly relied on 18 U.S.C. § 2703(d) – the same authority invoked in all three orders at issue in the present case – and that the Government was instead obliged under the Fourth Amendment to obtain a warrant based on probable cause. In a detailed opinion, the district court emphatically rejected this claim, holding instead that “cell site location records are the provider’s business records, and are not protected by the Fourth Amendment.” *Id.* at *12.

In a similar proceeding before this Court earlier this year, Judge Urbina reached the same conclusion:

In the instant case, as in *Smith*, the [cell-site location] information at issue was collected by the wireless cell phone service provider as the result of the defendant’s volitional choice to place a call. Under *Smith* then, no search took place because the defendant revealed information to a third party and therefore no longer had a reasonable expectation of privacy in that information. ...

In both *Smith* and this case, the information gathered revealed a suspect’s location (in the *Smith*’s [*sic*] case that the defendant was at home) and the numbers dialed. ... [T]his court is persuaded that under *Smith*, the government’s collection of CSLI pertaining to the defendant’s cell phone was not a Fourth Amendment “search.”

United States v. Gordon, Crim. No. 09-153-02 (RMU) at 2-3 (D.D.C. Feb. 6, 2012) (copy attached as Exhibit C).

The recent Sixth Circuit decision in *United States v. Skinner*, 2012 WL 3289801 (6th Cir. Aug. 14, 2012) underscores this reasoning, holding *Smith* applicable to precise GPS phone location data. *See id.* at *4. Given that the court of appeals found the Fourth Amendment inapplicable to a type of location information far more precise than the cell-site records at issue in this case,

defendant's claims here must be rejected *a fortiori*.

It is true that a tiny minority of courts have adopted a contrary view and concluded that cell-site location records enjoy constitutional protection.⁵ However, defendant overlooks the fact that one of the few cases he cites – *In re Application*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) (*Lenihan Opinion*) – was subsequently vacated by the Third Circuit, which rejected the lower court's unfounded constitutional claims and resolved the matter entirely on statutory grounds. *See In re Application*, 620 F.3d 304 (3d Cir. 2010).⁶

The lone remaining case cited by defendant – *In re Application*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (*Garaufis II Opinion*) – arose not in the context of a motion to suppress, but rather on an application where the court expressed uncertainty about the theoretical nature of the information that might be acquired. No such speculation is necessary in the present case: the Government has produced to defendant all of the cell-site location records obtained under the

⁵ Defendant mistakenly cites to two magistrate judge opinions – *In re Application*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (*Orenstein I Opinion*) and *In re Application*, 407 F. Supp. 2d 134 (D.D.C. 2006) (*Facciola Opinion*) – in support of his constitutional claim. Amici likewise erroneously rely upon *In re Application*, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) (*Peck Opinion*). *See* Brief Amici Curiae 4 n.2. None of these cases hold that the information in question enjoys Fourth Amendment protection. On the contrary, they hold only that there is no available statutory mechanism by which the Government may prospectively obtain cell-site location records, and that a warrant is the only available mechanism.

Notwithstanding the Government's disagreement with these courts on that statutory question, as discussed in Part C below this Court need not resolve the dispute: these cases are immaterial to defendant's present motion owing to the absence of any statutory suppression remedy.

⁶ Amici curiae commit the same error in citing *In re Application*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (*Orenstein II Opinion*). *See* Brief Amici Curiae 4 n.2. That magistrate judge decision was summarily reversed by the district court. *See* 2010 WL 5814659 (E.D.N.Y. Nov. 29, 2010).

challenged orders, and he is free to identify specific records that allegedly implicate the Fourth Amendment. Despite this, defendant and his supporting amici have failed to do so, offering instead only nebulous assertions about the hypothetical precision of the information that might have been acquired. This lack of specificity dooms defendant's claims. *See United States v. Karo*, 468 U.S. 705, 712 (1984) (“[W]e have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.”).

Defendant and amici likewise overlook the fact that the Chief Judge of this Court has held squarely that

a reasonable cellular phone customer presumably realizes that his calls are transmitted by nearby cell-site towers, and that cellular phone companies have access to and likely store data regarding the cell-site towers used to place a customer's calls. Thus, under *Smith*, CSLI constitutes information voluntarily rendered to a third-party cellular phone company, and government collection of that data from the third-party phone company is not a “search” under the Fourth Amendment.

In re Application, Misc. No. 11-449 (JMF/RCL) (D.D.C. Oct. 3, 2011) (*Lamberth Opinion*) (reversing Magistrate Judge Facciola's denial of the application) (redacted copy prepared by the Court attached as Exhibit D).⁷

Amici insist nevertheless that this court should ignore *Smith*, *Miller*, and their many progeny, and instead apply the reasoning of an opinion – *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) – establishing constitutional protections for email contents. Putting aside the fact that the Sixth

⁷ Although the matter before Chief Judge Lamberth involved access to cell-site location records for past time periods rather than prospective acquisition, that difference is inconsequential. Most obviously, *Smith* itself dealt with prospective surveillance (in the form of a pen register), and its logic – as well as Chief Judge Lamberth's application of it to historical cell-site location information – applies fully to the Government orders at issue here. And as noted above, there is no difference in the nature of the information so obtained; whether acquired prospectively or for historical periods, the records are identical in all respects.

Circuit has now spoken decisively in *Skinner*, amici fail to grasp the significant differences between this case and *Warshak*. Most obviously, the *Warshak* court placed great weight on the fact that “*Miller* involved simple business records, as opposed to the potentially unlimited variety of ‘confidential communications’” implicated by email. 631 F.3d at 288. But cell-site location records are “simple business records” generated by the technical operations of a cellular network, not the contents of confidential and intimate communications between two persons.

The Sixth Circuit distinguished *Miller* for a second reason: “the bank depositor in *Miller* conveyed information to the bank so that the bank could put the information to use ‘in the ordinary course of business.’ ... By contrast, [Warshak’s email service provider] was an intermediary, not the intended recipient of the emails.” *Id.* Here, however, the cell-site records generated by defendant’s use of his wireless phone were not meant for some third party, with the telephone company acting as a mere conduit. On the contrary, information about which cell tower the phone used to place and receive calls is integral to the process of providing wireless service, just as the bank in *Miller* actively processed and used the information conveyed to it (such as checks written by the customer). *See United States Telecomm. Ass’n v. FCC*, 227 F.3d 450, 463 (D.C. Cir. 2000) (signals sent from cell phones to cell sites “are necessary to achieve communications between the caller and the party he or she is calling”) (quoting brief of FCC). Given this crucial distinction, *Warshak* lends no support to defendant here, and provides no basis for abandoning the rule adopted by multiple members of this Court.

For all these reasons, this court should deny the motion. The federal courts have **unanimously** denied similar motions to suppress cell-site location records, and this Court should decline defendant’s invitation to take the unprecedented step of granting such a motion.

2. Even if analyzed under the Supreme Court’s cases concerning “tracking devices,” government access to cell-site location records is not a “search” and thus does not infringe any Fourth Amendment interest

As a business record in the possession of a third party, cell-site information should not be judged under Fourth Amendment standards applicable to tracking devices surreptitiously installed by the government. However, even measured against the constitutional standards articulated by the Supreme Court in this area, there is no reasonable expectation of privacy in cell-site information.

Defendant implies that *United States v. Karo*, 468 U.S. 705 (1984) entitles him to suppression. As explained below, this claim both misreads this precedent and overstates the accuracy of cell-site information, and the motion to suppress should thus be denied.

Contrary to the defendant’s argument, cell-site information provides only limited information about the location of a cell phone when a call is made. As one court has explained,

[t]he information does not provide a “virtual map” of the user’s location. The information does not pinpoint a user’s location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These 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.

Gorenstein Opinion, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005). Despite what the defendant and amici would like the court to believe, no precision location information, including GPS information, is contained in the records provided to the government here.⁸

Given that cell-site information is not precise, defendant is wrong that any constitutional privacy interest is at stake. In *Karo*, agents secretly installed a radio beeper in a can of chemicals,

⁸ In the same vein, amici erroneously imply that the records at issue in this case arose from “a mundane act – walking around with a cell phone turned on.” Brief Amici Curiae 11. In fact, each and every one of the records resulted directly from defendant’s intentional act of placing or answering a call.

and then tracked the can to various locations, including five separate residences and two multi-unit storage facilities. Where the tracking system enabled the government to locate the can of ether in a particular residence, the Supreme Court found that the Fourth Amendment had been infringed. 468 U.S. at 715. Conversely, the Court found no Fourth Amendment violation when the beeper was tracked to one of the storage facilities, but could not be tracked to the defendant's particular storage locker within the facility. *Id.* at 721, n.6. Because monitoring of the beeper could not be tracked to a particular locker and thus, revealed nothing about the inside of the defendant's locker, the Court held that monitoring did not result in a "search" of the locker. *Id.* at 721. As a result, the Court found no Fourth Amendment violation.

In sum, the test enunciated in *Karo* is not whether a tracked object is merely inside a constitutionally-protected private space. Rather, *Karo* holds that government use of a tracking device is a Fourth Amendment "search" only where the monitoring reveals the particular private location in which the tracked object may be found. Cell-site information, which is precise at its best only to within hundreds of yards, cannot disclose that a user's phone is inside a specific house or other constitutionally protected area.

Numerous courts addressing this issue with respect to prospective cell-site information have reached the same conclusion – that cell site information is not precise. In the words of one recent decision, "CSLI is less accurate than information obtained by GPS tracking technology Nor is there any indication in the record that CSLI is capable of distinguishing movements within a discrete space such as a residence." *Velasquez*, 2010 WL 4286276 at *5; *see also United States v. Madison*, 2012 WL 3095357 at *4 (S.D. Fla. July 30, 2012); *In re Application*, 2008 WL 5082506 at *5 (E.D.N.Y. Nov. 26, 2008) (*Garaufis I Opinion*) (cell-site information, "unlike the information

revealed by triangulation or ... Global Positioning System devices, is not precise enough to enable tracking of a telephone's movements within a home"); *In re Application*, 497 F. Supp. 2d 301, 311-12 (D.P.R. 2007) (*McGiverin Opinion*); *In re Application*, 411 F. Supp. 2d 678, 682 (W.D. La. 2006) (*Hornsby Opinion*) (“[C]ell-site information ... does not permit detailed tracking of a cell phone user within any residence or building. Indeed, the Government will not be able to pinpoint which room, house or building (if any) the user is in.”); *Gorenstein Opinion*, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005).

For this reason, courts have held that the Fourth Amendment is not implicated when the government obtains cell-site location information, and denied suppression motions as a result. *See Madison*, 2012 WL 3095357 at *9; *Velasquez*, 2010 WL 4286276 at *5; *United States v. Suarez-Blanca*, 2008 WL 4200156 (N.D. Ga. Mar. 26, 2008); *United States v. Flores*, 2007 WL 2904109 (N.D. Ga. Sept. 27, 2007); *Mitchell v. State*, 25 So. 3d 632 (Fla. Dist. Ct. App. 2009). For the same reasons, defendant's motion to suppress in this case should be denied.

3. Neither the D.C. Circuit's appellate decision in this case nor the Supreme Court's GPS tracking device decision compels a different result

Defendant suggests cursorily in his motion that the two appellate opinions previously issued in connection with this prosecution – both dealing with a GPS tracking device affixed to his vehicle, not with less-precise cell location records in the possession of a third party – support his claim of entitlement to suppression. He is mistaken.

Most importantly, the Supreme Court's opinion in *United States v. Jones*, 132 S. Ct. 945 (2012), holds only that when “the Government obtains information by physically intruding on a

constitutionally protected area, ... a search has undoubtedly occurred.” *Id.* at 951 n.3 (emphasis added). But when the Government merely compels a third-party service provider to produce routine business records in its custody, no physical intrusion occurs, and the rule in *Jones* is therefore wholly inapplicable.

Indeed, at least five different courts have held that *Jones* is irrelevant to the acquisition of cell phone location records from a service provider. See *United States v. Skinner*, 2012 WL 3289801 at *6 (6th Cir. Aug. 14, 2012) (“No such physical intrusion occurred in Skinner’s case.”); *Garcia v. Bradt*, 2102 WL 3027780 (S.D.N.Y. July 23, 2012) (denying habeas petition because, *inter alia*, the allegedly improper acquisition of phone location records involved “no such physical occupation of petitioner’s property”); *In re Application*, 2012 WL 989638 (D. Mass. Mar. 23, 2012) (*Collings Opinion*) (granting Government’s application “because the Court Order allowing the government to obtain the [cell-site location] records does not involve any attachment of any device on any of an individual’s real or personal property”); *Graham*, 2012 WL 691531 at *10 (*Jones* inapplicable because compelled production of cell-site location records “does not involve a physical trespass to property”); *Gordon*, Exh. C at 2-3 (expressly rejecting *Jones*-based motion to suppress cell-site location records).

Defendant’s attempted reliance on *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), fares no better. To begin with, it is unclear that the D.C. Circuit’s “mosaic theory” – under which the sum total of individual non-search acts eventually aggregates into a totality implicating the Fourth Amendment – even survives *Jones*. Speaking directly to Justice Alito’s concurrence suggesting a constitutional distinction between short-term GPS vehicle tracking and longer-term monitoring, the *Jones* majority

dismissed that as a “novelty” whose basis “remains unexplained.” 132 S. Ct. at 954.⁹

But even assuming that *Maynard*’s mosaic theory remains valid at all, this Court should reject the attempt to expand its reach outside of GPS tracking of vehicles. Most obviously, GPS location information is far more precise than cell-site location information, so the latter does not provide an “intimate portrait” of a person’s activities of the sort that troubled the *Maynard* court. Moreover, the GPS tracking at issue in *Maynard* involved no volitional acts by the defendant; cell-site location records, by contrast, are not generated 24/7 at the Government’s discretion, but rather come into existence only when a user makes an affirmative choice to use his phone to initiate or receive a communication.

Both Chief Judge Lamberth and Judge Urbina of this Court have expressly endorsed these key distinctions and refused to apply the mosaic theory to cell-site location records. As Judge Urbina

⁹ Justice Sotomayor’s concurrence in *Jones* did observe that 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. But the concurrence made it clear that answering that question was “unnecessary” to resolving the issue in *Jones*. *Id.* To disregard the venerable precedent of *Smith* on the basis of a single Justice’s concurrence would ignore the Supreme Court’s admonition that “if a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the [lower courts] should follow the case which directly controls, leaving this Court the prerogative of overruling its own decisions.” *Agnostini v. Felton*, 521 U.S. 203, 237 (1997) (citations omitted). Even when there is reason to think that evolving Supreme Court authority has substantially undermined a binding Supreme Court precedent, a motion based on that evolution, must “be denied unless and until [the Supreme] Court reinterpret[s] the binding precedent.” *Id.* at 238.

Several courts have followed this guidance in refusing to apply the rules urged in the *Jones* concurrences. *See Gordon*, Exh.C at 2 (“Notwithstanding the vivid discussion by both Justice Sotomayor and Justice Alito, the *Jones* Court did not reconsider the fundamental principle articulated in *Smith*, and this court therefore remains bound by it.”); *Collings Opinion*, 2012 WL 989638 at *1-*2 (granting two applications for 7 months and 6 weeks, respectively, of historical cell-site records); *Graham*, 2012 WL 691531 at *15-*16 (noting that *Jones* majority “did not endorse the D.C. Circuit’s mosaic theory” and discussing several doctrinal problems with that theory; rejects motion to suppress 221 days’ worth of historical cell location records).

observed in *Gordon*,

[s]uch information is not comparable to the GPS information at stake in *Jones*, which included tracking Jones for twenty-four hours a day, seven days a week no matter his activities or choices. CSLI does not ... provide a complete record of the cell phone location, instead revealing only the cell phone user's approximate location at the time that he placed a call.

Exh. C at 3. Likewise, Chief Judge Lamberth held late last year, in reversing Magistrate Judge Facciola's denial of a government application for cell-site location records, that

CSLI ... differs in important respects from the GPS tracking involved in *Maynard*. ... Disclosure of historical CSLI for limited numbers of specific calls ... does not paint such a detailed portrait of an individual's life. Historical CSLI like that sought by the government here does not provide a record of a cell phone user's each and every destination, or the length of time he remains there. Instead, historical CSLI reveals only an approximate position from which a user placed a call, and is silent as to the duration spent in transit from one place to another. Like a blank connect-the-dot image, historical CSLI comprises an incomplete and scattershot image of an individual's travels, lacking sufficient detail to provide the "intimate picture" envisioned in *Maynard*. They thus do not amount to the sort of intrusion on privacy that under *Maynard* implicates the Fourth Amendment.

Lamberth Opinion, Exh. D at 11. And although Chief Judge Lamberth suggests that cell-site location records covering "a more prolonged period of time" would "present a closer question," *id.* n.6, the facts here do not justify a contrary result, especially given that the Government sought judicial authorization (and thus subjected itself to this Court's continuing oversight) not merely once, but three separate times at roughly six-week intervals. *See Graham*, 2012 WL 691531 at *7 (finding "important" the distinction between *Maynard*, involving no judicial authorization, and the judicial oversight contemplated under section 2703; refusing to suppress 221 days' worth of cell-site location records).

This Court should decline to expand the mosaic theory beyond the facts of *Maynard/Jones* for another reason: under the argument made by amici, almost any criminal investigative activity –

however routine or based in longstanding common-law or statutory authority – can become a cumulative “search” at some point unknowable except in hindsight. As the *Graham* court notes,

using only ordinary investigatory techniques, police can (and do) collect vast amounts of data on criminal suspects. After interviewing witnesses, conducting surveillance (perhaps enhanced by discrete requests for historical cell site location records under the Stored Communications Act), and reviewing pen registers and bank records, police may be able to paint an “intimate picture,” *Maynard*, 615 F.3d at 562, of a person's life. Under the mosaic theory, at some point this collection of data would become a Fourth Amendment search at some undefined point.

846 F. Supp. 2d at 402. Extending the mosaic theory to third-party records would open up a doctrinal Pandora’s Box, unduly inhibiting investigators and putting this Court in the position of having to assess, in every future criminal case, whether the government’s collection of telephone toll records, bank account records, and other documentary evidence went on “too long” or revealed “too much” according to some indefinite standard. (This, of course, despite the fact that the objective in almost every criminal investigation is to develop a picture of a suspect’s activities, associations, and motivations, not only to sustain the government’s heavy trial burden of proof but also to ensure that the guilty are punished and to avoid mistaken prosecution of innocent persons.) The adverse consequences would be profound, and this Court should instead join Chief Judge Lamberth and Judge Urbina in soundly rejecting expansion of the mosaic theory.

For all of these reasons, this Court should deny the motion to suppress.

B. The Government’s good-faith reliance upon judicial and statutory authorization, as well as binding appellate precedent, precludes suppression of the evidence

Even if this Court were to conclude, contrary to the overwhelming weight of authority cited above, that the Fourth Amendment protects the third-party records at issue in this case, defendant

would still not be entitled to the extraordinary remedy of suppression. “The fact that a Fourth Amendment violation occurred ... does not necessarily mean that the exclusionary rule applies.” *Herring v. United States*, 555 U.S. 135, 140 (2009). On the contrary, exclusion of evidence is appropriate only where it would have a substantial deterrent effect, and even then only when weighed against the heavy cost to society and the truth-seeking function. *Id.*

In particular, the Supreme Court has ruled squarely that an officer’s reasonable reliance on a statute – even where a court concludes in hindsight that the statute is constitutionally infirm – bars application of the exclusionary rule. In *Illinois v. Krull*, 480 U.S. 340 (1987), the Supreme Court held that “[p]enalizing the officer for the [legislature’s] error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.” *Id.* at 350. Such reliance on a duly enacted statute is unreasonable only “if, in passing the statute, the legislature wholly abandoned its responsibility to enact constitutional laws.” *Id.* at 355. Absent the patent unconstitutionality of such a statute, an officer’s good-faith reliance on it may not be penalized through suppression of evidence.

The agents in this case relied upon just such a statute, 18 U.S.C. § 2703(d), the applicability of which the defendant here concedes. *See* Def. Mem. at 4. As detailed in Part C below, not only did investigators here comply with this Congressional enactment, but the overwhelming weight of judicial authority holds that a) the statute may be used to compel cell-site records possessed by a third-party provider and b) such compulsion in no way intrudes upon a Fourth Amendment interest. Under these circumstances, the investigators’ reliance on the statute in this case was anything but unreasonable, and therefore falls squarely within the rule articulated in *Krull*. As another court has held expressly,

it was objectively reasonable for law enforcement to rely on [section 2703(d)] to

obtain historical cell site information because some case law suggests that [section 2703(d)] applies to the historical cell site information and there was not much case law that questioned the constitutionality of [section 2703(d)] for historical cell site information at the time that the government sought approval for obtaining the historical cell site information.

Suarez-Blanca, 2008 WL 4200156 at *12 (N.D. Ga. Apr. 21, 2008) (denying suppression).

Although some of the Magistrate Judges of this Court (such as Magistrate Judge Facciola) subsequently concluded – wrongly, in our view – that the Government could not acquire prospective cell-site locations records via the statutory mechanism relied on here, those decisions post-dated all three of the orders at issue in this motion. Indeed, two of the orders (June 20 and September 19, 2005) were signed by Magistrate Judge Facciola himself.

Notably, the reliance in *Krull* itself (on a statute that authorized warrantless administrative searches) involved no *ex ante* judicial ratification. In this case, by contrast, the Government relied not only on a statute, but also on this Court’s issuance of three separate orders. In the recent *Graham* case, the district court identified this as a separate basis for denying a motion to suppress cell-site location records, applying the rationale of *United States v. Leon*, 468 U.S. 897 (1984). *See Graham*, 2012 WL 691531 at *19-*20. Just as in that case “it was objectively reasonable for law enforcement to rely” on the two magistrate judges’ orders, *id.* at *19, so too it was reasonable here, with the result that the evidence may not be excluded.

A third basis for finding good-faith reliance – and thus denying defendant’s motion – resides in *Davis v. United States*, 131 S. Ct. 2419 (2011), where the Supreme Court held that searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule. *Davis* presented the Court with the issue of whether the fruits of police actions in searching a car, which were proper at the time under that Circuit's precedent interpreting *New York*

v. Belton, would nonetheless be subject to the exclusionary rule because the actions violated the Fourth Amendment under the recent decision of *Arizona v. Gant*. The Court reasoned that the remedy of exclusion does not automatically follow from a Fourth Amendment violation and that because law enforcement's actions complied with then-existing binding precedent, suppression was not appropriate.

Here, the cell-site data was in the hands of a third party and thus under the prospective-surveillance precedent of *Smith*, no warrant was necessary to acquire that information. Even if the Supreme Court's opinion in *Jones* had somehow undermined or limited *Smith* – which it did not¹⁰ – that fact would be irrelevant to assessing the reasonableness of the Government's reliance on *Smith* a full seven years ago when the orders in this case first issued. As a result, this Court should deny defendant's motion to suppress the challenged cell-site records.

C. The government obtained cell-site information lawfully in this case, and in any event the evidence is not subject to suppression under any statutory theory

In his brief, the defendant concedes that 18 U.S.C. § 2703(d) “permits the government to obtain an order seeking the cell- site-location [*sic*] records at issue here.” Deft. Mem. at 4. Despite this concession, he asserts that the government failed to make the required factual showing in support of its application, and that this purported failure entitles him to suppression of the disputed records.

Defendant is doubly incorrect. First, the government made the necessary showing. More

¹⁰ As Judge Urbina recently held in *Gordon*, “the *Jones* Court did not reconsider the fundamental principle articulated in *Smith*, and this court therefore remains bound by it.” Exh. C at 2.

importantly, even if the government had failed to do so, no statutory suppression remedy exists. For that reason, no federal court has ever ordered the statutory suppression of cell-site records; on the contrary, numerous courts have denied such motions and emphatically rejected the arguments put forward by the defendant.

1. The government properly obtained records concerning defendant's phone using a court order under 18 U.S.C. § 2703(d)

As noted above, defendant concedes that 18 U.S.C. § 2703(d) “permits the government to obtain an order seeking the cell- site-location [*sic*] records at issue here.” Deft. Mem. at 4. We agree, as have numerous courts, including the Third Circuit. *See, e.g., In re Application*, 620 F.3d 304, 313 (3d Cir. 2010) (“In sum, we hold that [cell-site location information] from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination.”); *Gorenstein Opinion*, 405 F. Supp.2d 435, 444 (S.D.N.Y. 2005) (noting that cell-site data is “information” and “pertain[s] to a subscriber to or customer of cellular telephone service”).¹¹

However, defendant does challenge the adequacy of the “specific and articulable” facts

¹¹ As amici argue in Part II of their brief, it is true that a few courts have rejected the Government’s position that it may obtain cell-site location records prospectively in reliance on section 2703(d) and the pen register statute (sometimes described as the “hybrid theory”). *Compare Garaufis II Opinion*, 2009 WL 1594003 (E.D.N.Y. Feb. 26, 2009) (endorsing government’s position); 2007 WL 397129 (E.D. Cal. Feb. 1, 2007) (*Hollows Opinion*) (same); and *In re Application*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (*Kaplan Opinion*) (same) with *In re Application*, 2009 WL 8231744 (E.D. Ky. Apr. 17, 2009) (*Wier Opinion*) (rejecting “hybrid theory”); *McGiverin Opinion*, 497 F. Supp. 2d 301 (D.P.R. 2007) (same); and *Facciola Opinion*, 407 F. Supp. 2d 134 (D.D.C. 2006) (same). This court need not resolve this disagreement in addressing the pending motion to suppress because, as discussed below, there is in any event no applicable statutory suppression remedy.

provided in these particular applications. This argument disregards the fact that the applications stated that there was “reliable information” to believe that the target cellular telephone was being used to further “a conspiracy to distribute and to possess with intent to distribute narcotic controlled substances” (Applications at Para. 2), and that cell-site information associated with use of the phone would have significant investigative value (*id.* Para. 10).

As the 1994 House Judiciary Committee report for the legislation that established the “specific and articulable facts” standard makes clear, this is “an intermediate standard ... higher than a subpoena, but not a probable cause warrant.” H. Rep. No. 827, 103d Cong., 2d Sess. 31 (1994) (emphasis added), reprinted in 1994 U.S. Code Cong. & Admin. News 3489, 3511; *see also In re Application*, 620 F.3d 304, 314 (3d Cir. 2010) (same). Two Magistrate Judges of this Court found that the Government’s applications in this case satisfied this standard, and their assessment is entitled to considerable deference. *Cf. Illinois v. Gates*, 462 U.S. 213, 236 (1983) (“A magistrate’s ‘determination of probable cause should be paid great deference by reviewing courts.’”) (citation omitted).

2. The Stored Communications Act provides no statutory suppression remedy

More importantly, even if the government’s use of section 2703(d) in this case were improper, suppression is not available as a remedy. None of the cases cited by defendant – including the now-vacated *Lenihan Opinion* from the Western District of Pennsylvania – granted suppression or supports such a remedy, and no such remedy is available. *See* 18 U.S.C. § 2708 (“The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.”).

To the contrary, courts have unanimously held that no such statutory suppression remedy exists under the Stored Communications Act. *See United States v. Powell*, 2011 WL 4037404 at *2 (3d Cir. Sept. 13, 2011) (unpublished); *United States v. Clenney*, 631 F.3d 658, 667 (4th Cir. 2011); *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) (“the Stored Communications Act expressly rules out exclusion as a remedy”); *United States v. Christie*, 2009 WL 742720 at *3 (D.N.J. Mar. 18, 2009); *United States v. Wellman*, 2009 WL 37184 at *8 n.2 (S.D. W. Va. Jan. 7, 2009); *United States v. Qing Li*, 2008 WL 789899 at *3 (S.D. Cal. Mar. 20, 2008); *United States v. Beckett*, 544 F. Supp. 2d 1346, 1350 (S.D. Fla. 2008); *United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); *Bansal v. Russ*, 513 F. Supp. 2d 264, 282-83 (E.D. Pa. 2007); *United States v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (“[S]uppression is not a remedy contemplated under the ECPA.”); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) (“Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act.”), *aff’d*, 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000); *United States v. Reyes*, 922 F. Supp. 818, 838 (S.D.N.Y. 1996) (“Exclusion of the evidence is not an available remedy for this violation of the ECPA.”). Courts have applied this general principle in the specific context of cell-site records. *See Powell*, 2011 WL 4037404 at *2; *Suarez-Blanca*, 2008 WL 4200156 at *4 (holding that suppression is not a remedy for asserted violations of the SCA, and rejecting a defense motion to exclude cell-site location information).

In four of the above-listed cases – *Powell*, *Perrine*, *Ferguson*, and *Kennedy* – the issue was precisely the one raised by defendant in the instant case – whether the government satisfied the

“specific and articulable facts” standard of 2703(d). In each of those cases, the court found that suppression was not available. Thus, as the Third Circuit observed last year, “even if Powell had shown a violation of the statute, exclusion [of the challenged cell-site location records] would not be the appropriate remedy.” 2011 WL 4037404 at *2.

Accordingly, even if defendant were correct that the order violated 18 U.S.C. § 2703(d) because the applications failed to set forth “specific and articulable facts,” that argument cannot sustain a motion to suppress. Defendant’s motion must therefore be denied.

CONCLUSION

For the reasons set forth above, the government respectfully requests that defendant’s motion to suppress be denied.

Respectfully submitted,

RONALD C. MACHEN JR.,
Bar No. 447889
United States Attorney

_____/S/_____
Arvind K. Lal, Bar # 389489
Darlene M. Soltys, Bar # 431036
Courtney D. Spivey, N.Y. Bar
Assistant United States Attorneys
Mark Eckenwiler, N.Y. Bar
Associate Director,
Dept. Of Justice, Office of Enforcement Operations
United States Attorneys Office
555 4th Street, N.W., Room 4106 (Lal)
Washington, DC 20530