IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,	*	
V.	*	
AARON GRAHAM,	*	CRIMINAL NO.: RDB-11-0094
AND		
ERIC JORDAN	*	
DEFENDANTS	*	

* * * * * * * * * * * * *

MEMORANDUM OPINION

Defendants Aaron Graham and Eric Jordan (collectively "Defendants") are charged in a seventeen-count Second Superseding Indictment relating to a series of armed Hobbs Act[1] robberies committed in Baltimore City and Baltimore County, Maryland in January and February 2011. The Defendants filed numerous pre-trial motions, including a variety of motions to suppress. Over the course of five separate days, this Court heard argument and ruled on all but one of the motions to suppress. The only remaining pending motion is Defendant Graham's Motion to Suppress Cellular Phone Data and Historical Cell Site Location Data, which Defendant Jordan has joined. On December 8, 2011, this Court held a hearing devoted entirely to this issue. During the pendency of this motion, this Court allowed supplemental briefing, and after the December 8 hearing, ordered further briefing.[2]

[1] Title 18, United States Code, Section 1951.

[2] As will be discussed *infra*, the Supreme Court of the United States recently issued an opinion that is relevant but not controlling in this case, *United States v. Jones*, 565 U.S. __, No. 10-1259, slip op. (January 23, 2012). *See infra* n.6, and discussion throughout. This Court did not order further briefing regarding the implications of that case insofar as further briefing would not aid this Court's decision.

For the reasons that follow, the Defendants' Motion to Suppress Historical Cell Site Location Data (ECF No. 38) is DENIED.

BACKGROUND

The Second Superseding Indictment in this case (ECF No. 16) charges the Defendants with conspiring to rob and robbing a variety of commercial entities, including a Burger King restaurant and a McDonald's restaurant, both located in Baltimore City, Maryland.[3] Both robberies took place in the afternoon hours of February 5, 2011. Witnesses at both robberies provided descriptions of the robber and the get-away vehicle to the responding officers. The witnesses indicated that the robber wore a red, gray, and black North Face jacket, and upon exiting the restaurants, was driven away in a dark gray Ford F-150 pickup truck that was being operated by a second person. Approximately ten minutes after the McDonald's robbery, the Defendants were apprehended in a vehicle that matched the description given by the witnesses, and Defendant Graham was wearing a matching jacket. A handgun and United States currency was recovered from the Defendants and from the vehicle. Both Graham and Jordan provided their cellular telephone numbers to the arresting officers.

Two cellular telephones were recovered from the Ford pickup truck—a blue Samsung and a silver Sanyo. Prior to searching the contents of the phones, Baltimore City Police Detective Christopher Woerner sought and obtained search warrants for the two phones in the Circuit Court for Baltimore City. *See* Gov. Opp'n at 7, ECF No. 49; Warrants,

[3] In addition to the Hobbs Act robbery charges, 18 U.S.C. § 1951, the Defendants are also charged with being felons in possession of a firearm in violation of 18 U.S.C. § 922(g), and with possessing firearms in furtherance of a crime of violence in violation of 18 U.S.C. § 924(c).

ECF Nos. 49-4 & 49-5. The telephone number associated with the Samsung phone matched the number that Defendant Graham provided to investigators, and the number associated with the Sanyo phone matched the number provided by Defendant Jordan.

Federal authorities initially charged the Defendants with only firearm violations. However, an investigation into the Baltimore City robberies and other Baltimore County robberies was ongoing, and on March 25, 2011, the government applied for an order from Magistrate Judge Susan K. Gauvey of this Court, pursuant to the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.*, which ordered Sprint/Nextel, Inc. to disclose to the government "the identification and address of cellular towers (cell site locations) related to the use of [the Defendants' cellular telephones]." SCA App. 1, ECF No. 49-9. The government sought cell site location data for the periods of August 10-15, 2010; September 18-20, 2010; January 21-23, 2011; and February 4-5, 2011. *Id.* In its application, the government alleged that the information sought was relevant to an ongoing criminal investigation regarding the Burger King and McDonald's robberies, as well as several other prior robberies that the Defendants were suspected of committing. By identifying the location of cellular towers accessed by the Defendants' phones during the relevant time periods, the government sought to more conclusively link the Defendants with the prior robberies.

On March 25, 2011, Magistrate Judge Gauvey granted the government's application. Specifically, Magistrate Judge Gauvey applied the well-defined standard prescribed by the Stored Communications Act and made a factual finding that the government "offered specific and articulable facts showing that there are reasonable grounds to believe that the

records and other information sought are relevant and material to an ongoing criminal investigation." *Id.* at 8. The original indictment against the Defendants was subsequently superseded to include the Baltimore City robberies.

While the investigation into the Baltimore City robberies was ongoing, the government was presented with evidence regarding additional related robberies in Baltimore County. In connection with this investigation, the Grand Jury returned a Second Superseding Indictment on May 18, 2011 to include the Baltimore County robberies. The government had not included the time periods for these robberies in its initial application for cell site location data, and so, on July 8, 2011, submitted a second application for cell site data, this time with Magistrate Judge Paul W. Grimm of this Court for the time period of July 1, 2010 through February 6, 2011. SCA App. 2, ECF No. 49-10. This application sought all the data acquired as part of the first Stored Communications Act order, as well as for additional time periods not previously covered. Finding that the government had offered specific and articulable facts in support of the application as required by the Stored Communications Act, Magistrate Judge Grimm approved the application on July 15, 2011. *See id.* at 8-9. Sprint/Nextel, Inc. complied with the orders, and provided the requested data to the government.[4]

[4] In its papers, and at the hearing conducted on December 8, 2011, the government advised that it had analyzed the data obtained via the first application, but had not yet analyzed any of the data obtained pursuant to the second application. *See* Gov. Surreply at 3, ECF No. 55.

ANALYSIS

The Defendants argue that the government's acquisition of historical cell site location data, without a warrant but pursuant to the Stored Communications Act, was in violation of their Fourth Amendment rights and must be suppressed. The Defendants do not argue that the Stored Communications Act is unconstitutional on its face, but instead make an as-applied challenge and contend that the length of time and extent of the cellular phone monitoring conducted in this case intruded on the Defendants' expectation of privacy and was therefore unconstitutional. Essentially, the Defendants present the question of whether twenty-four hour "dragnet" surveillance by emerging technological means infringes on the Fourth Amendment's guarantee against unreasonable searches and seizures. *See* Defs. Reply at 1, 4, ECF No. 51 (quoting *United States v. Knotts*, 460 U.S. 276, 283-84 (1983)).

More specifically, the Defendants argue that Magistrate Judge Gauvey's March 25, 2011 Order, which authorized the release of fourteen days and 1,628 individual cell site location data points, and Magistrate Judge Grimm's July 15, 2011 Order, which authorized two hundred and twenty-one days and 20,235 individual cell site location data points, infringed on the Defendants' expectations of privacy insofar as that data allows the government to paint an intimate picture of the Defendants' whereabouts over an extensive period of time. While the Defendants do not take issue with any specific data points, they essentially argue that the privacy intrusions available through this type of technology are far reaching and unconstitutional—allowing the government to retroactively track or surveil a suspect through his cellular telephone, a device he likely carries with him at all hours of the day and to constitutionally protected places such as his home or church.

The government makes four arguments in response. First, the government contends that the Defendants lack standing to challenge the seizure of the historical cell site location records from Sprint/Nextel, Inc. In this regard, the government argues that Defendant Jordan's use of a fictitious name and address in subscribing to the cellular phone service evidences a lack of privacy or possessory interest in the phone and the underlying location records.[5] Moreover, the government argues that neither Defendant has standing insofar as the actual records are the proprietary business records of Sprint/Nextel, Inc. and were voluntarily conveyed by the Defendants to the cellular service company.

Second, and relatedly, the government expands on its business records argument, and contends that the Defendants have no Fourth Amendment expectation of privacy in business records voluntarily conveyed to a third party. Analogizing from Supreme Court precedent, the government argues that the voluntary disclosure of cell site location data is akin to dialed telephone numbers captured by pen registers and bank records disclosed to banks—which the Court has found do not implicate the Fourth Amendment. Under this so-called "third-party doctrine," the government maintains that by using their cellular phones, and thereby voluntarily conveying their approximate location to their service provider, the Defendants can claim no legitimate expectation of privacy in that data—in other words, the Fourth Amendment simply does not apply.

Third, the government argues that an application for historical cell site location data does not require probable cause—rather, the Stored Communications Act's lower "specific

[5] The government does not make this argument for Defendant Graham insofar as his cellular phone was subscribed in the name of Mr. Graham's wife, and the address associated with the subscription matches that used by Mr. Graham prior to his arrest.

and articulable facts" standard provides adequate privacy protections, and the disclosure of such information does not run afoul of the Fourth Amendment. Notwithstanding some recent cases to the contrary, the government maintains that the majority of courts to consider the issue have concluded that the government's acquisition of cell site location data without a warrant does not violate the Fourth Amendment.

Finally, the government argues that even if this Court concludes that a warrant was required for the acquisition of the location data in this case, and that the Defendants' Fourth Amendment rights were violated, the remedy for such a violation is not the suppression of the evidence. In this regard, the government contends that law enforcement officers in this case justifiably, and in good faith, relied on the Stored Communications Act and two court orders that relied on that statute.

While the central issue presented, *i.e.*, whether a defendant's Fourth Amendment rights are violated when the government acquires historical cell site location data without a warrant based on probable cause, is one of first impression in this district and in the Fourth Circuit, it is not altogether novel. In light of the expanding use of cellular network information by law enforcement, several courts have recently grappled with the Fourth Amendment implications of cellular phone technology that allow law enforcement to approximate the location of suspects' cellular phones—and by implication, the location of the suspects themselves.

Some courts, most notably the Eastern District of New York and the Southern District of Texas, have concluded that, under certain circumstances, applications seeking cell site location data must be granted only after a showing of probable cause, and not the lower

statutory standard of "specific and articulable facts" contained in the Stored Communications Act. *See, e.g.*, *In re Application of the United States*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (Garaufis, J.); *In re Application of the United States*, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (Smith, Mag. J.), *appeal docketed*, No. 11-20554 (5th Cir. Dec. 14, 2011); *In re Application of the United States*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (Orenstein, Mag. J.), *rev'd* No. 10-MC-0550 (E.D.N.Y. Nov. 29, 2011) (unpublished order noting written opinion to follow). Those courts have essentially held that a government application for cell site location records does not implicate the Fourth Amendment if the request is for a discrete, and relatively short period of time. *Compare In re Application*, 736 F. Supp. 2d at 578-79 (application requesting cell site location data for a period of 58 days required warrant based on probable cause); *In re Application*, 747 F. Supp. 2d at 829 (60 days), *with In re Application of the United States*, No. 11-MC-0113, 2011 WL 679925, at *1 (E.D.N.Y. Feb. 6, 2011) (application for a period of 21 days required only specific and articulable facts, and not probable cause). In other words, those courts have concluded that the Fourth Amendment is only implicated when the government surveillance of historical cell site location data occurs over a sufficiently long—albeit undefined—period of time so as to implicate a person's legitimate expectation of privacy. None of these decisions have explicitly defined the length of time at which a request for cell site location data must be supported by probable cause, but Magistrate Judge Orenstein of the Eastern District of New York suggested that thirty days might be an appropriate limit. *See In re Application*, 2011 WL 679925, at *2.

A majority of courts, on the other hand, have concluded that the acquisition of historical cell site location data pursuant to the Stored Communications Act's specific and articulable facts standard does not implicate the Fourth Amendment, regardless of the time period involved. *See, e.g.*, *United States v. Dye*, No. 10CR221, 2011 WL 1595255, at *9 (N.D. Ohio Apr. 27, 2011); *United States v. Velasquez*, No. 08-730-WHA, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010); *United States v. Benford*, No. 09 CR 86, 2010 WL 1266507, at *3 (N.D. Ind. Mar. 26, 2010); *United States v. Suarez-Blanca*, No. 07-023-MHS/AJB, 2008 WL 4200156, at *8-11 (N.D. Ga. Apr. 21, 2008); *In re Application of the United States*, 509 F. Supp. 2d 76, 80-81 (D. Mass. 2007). These courts have primarily relied on a line of Supreme Court cases construing the scope of Fourth Amendment rights relating to business records held by third parties. More specifically, these courts have concluded that because people voluntarily convey their cell site location data to their cellular providers, they relinquish any expectation of privacy over those records. *See Suarez-Blanca*, 2008 WL 4200156, at *8 (finding no expectation of privacy in records kept by third parties) (citing, *inter alia*, *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435, 442-44 (1976)).

For the following reasons, this Court concludes that the Defendants in this case do not have a legitimate expectation of privacy in the historical cell site location records acquired by the government. These records, created by cellular providers in the ordinary course of business, indicate the cellular towers to which a cellular phone connects, and by extension the approximate location of the cellular phone. While the implications of law enforcement's use of this historical cell site location data raise the specter of prolonged and constant government surveillance, Congress in enacting the Stored Communications Act,

has chosen to require only "specific and articulable facts" in support of a government application for such records. Put simply, the Fourth Amendment, as currently interpreted, does not contemplate a situation where government surveillance becomes a "search" only after some specified amount of time.[6]

Accordingly, and in light of the difficult question presented and the differing conclusions reached by other courts, this Court finds that the Stored Communications Act, as drafted, provides adequate privacy protections for historical cell site location data—and if the arc of technological improvement (or the implementation of that technology by the government) should be altered in a way that does infringe a person's legitimate expectation of privacy, the solution is properly for the legislature to address. *See United States v. Jones*, 565 U.S. __, No. 10-1259, slip op. at 13 (January 23, 2012) (Alito, J. concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.") (citation omitted).

[6] Recently, the Supreme Court of the United States issued an opinion holding that the surreptitious installation of a global positioning system ("GPS") device on a suspect's vehicle constitutes a "search" under the Fourth Amendment. *See United States v. Jones*, 565 U.S. __, No. 10-1259, slip op. at 3 (January 23, 2012). While the majority opinion in *Jones* went no further, as will be discussed, at least four justices, *see infra* n.15, appeared ready to embrace an interpretation of the Fourth Amendment that would require a showing or probable cause when government surveillance occurred over a sufficiently prolonged period of time. *See id.* at 13 (Alito, J. concurring).

I. THE FOURTH AMENDMENT & HISTORICAL CELL SITE DATA

At the outset, it is important to define precisely what privacy interests the Defendants claim were infringed in this case. In their own words, the Defendants argue that "[w]here intermittent periods of constant cell location surveillance reveal the patterns of a person['s] movements, that person's privacy has been severely compromised." Defs. Reply at 5, ECF No. 51. Implicit in this argument, is the idea that surveillance in and of itself does not necessarily implicate Fourth Amendment privacy concerns, but in the aggregate, some amount of cellular location data gathering will eventually run afoul of the Constitution.

As previously mentioned, several courts have recently concluded that government acquisition of historical cell site location data over a prolonged period of time can violate the Fourth Amendment if not acquired pursuant to a warrant supported by probable cause. *See, e.g.*, *In re Application of the United States*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011) (Garaufis, J.) *In re Application of the United States*, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (Smith, Mag. J.), *appeal docketed*, No. 11-20884 (5th Cir. Dec. 14, 2011); *In re Application of the United States*, 736 F. Supp. 2d 578 (E.D.N.Y. 2010) (Orenstein, Mag. J.), *rev'd* No. 10-MC-0550 (E.D.N.Y. Nov. 29, 2011) (unpublished order noting written opinion to follow).

Undergirding the reasoning of each of these cases is *United States v. Maynard*, a case decided by the United States Court of Appeals for the District of Columbia Circuit in August, 2010. 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 565 U.S. __, No. 10-1259, 2012 WL 171117, (January 23, 2012). The Circuit Court in *Maynard* held that government use of a GPS device installed on a suspect's car to monitor the suspect's location on public roads constitutes a Fourth Amendment "search" when the surveillance is

conducted over a long period of time—in that case, a month. *Id.* at 558-62. In making this determination, the D.C. Circuit essentially created a new "mosaic" theory of the Fourth Amendment in which individual investigatory steps taken by law enforcement do not amount to a Fourth Amendment violation, but when viewed in the aggregate—for example constant twenty-four hour GPS surveillance over the course of a month—infringe on a person's reasonable expectations of privacy. *See id.* at 562. In this regard, the *Maynard* court concluded that:

> [W]e hold the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.

Id. at 560.

Of course, *Maynard* concerned the prolonged surveillance of a vehicle by global positioning system technology, and not through historical cell site location data. That distinction is important. Historical cell site location data, is, as its name implies, historical—the information revealed by such data exposes to the government only where a suspect *was*

and not where he *is*.[7] The GPS technology at issue in *Maynard*, on the other hand, revealed to the government the location and movements of the suspect in real time. *See id.* at 558 ("the police used the GPS device . . . to track Jones's movements 24 hours a day for 28 days *as* he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place.") (emphasis added). Also, the GPS location data at issue in *Maynard* was far more precise than the historical cell site location data at issue here.

---

[7] Recently, Magistrate Judge Gauvey of this Court issued an opinion in which she considered the government's application for a search warrant seeking a suspect's precise location through real-time cellular site location and GPS technology. *See In re Application of the United States*, __ F. Supp. 2d __, No. 10-2188-SKG, 2011 WL 3423370 (D. Md. Aug. 3, 2011). In that case, the government had an arrest warrant for a suspect in a crime, and they had the suspect's cellular telephone number. The government sought a warrant directing the cellular provider to disclose the precise location of the suspect's telephone (in real time) in order to effectuate the arrest of the suspect. Magistrate Judge Gauvey declined to issue the warrant on the ground that the Fourth Amendment does not provide the authority for a search warrant requesting location data to aid in the apprehension of a subject of an arrest warrant. *See id.* at *24-30. However, in making this ruling, Magistrate Judge Gauvey expressly differentiated between real-time or *prospective* location data and *historical* cell site location data:

> The kind of location information that is most commonly sought under § 2703 [of the Stored Communications Act] is cell site data—information that is automatically collected by cell sites as a user's handset "checks in" or "registers" with the network. In the *least invasive* of this type of search, the government will request historic cell site information that was routinely recorded by a single cell site and retained by the carrier when a handset user placed or received calls *prior* to the issuance of an order or warrant. In a *more invasive* search, the government will request that the carrier retain records for all of a handset's automatic registrations, which occur approximately every seven to ten minutes. Such a request is *prospective*, as it asks for data generated *after* the court's order or warrant and involves data being generated and turned over to law enforcement in real time, or close to it. As discussed above, this data is available only when a handset is powered on and is able to access its network. And, importantly, these requests involve data that is automatically generated by use of any cell phone and is "intermediat[ly] stor[ed] . . . incidental to the electronic transmission thereof." 18 U.S.C. §§ 2703, 2711(1), 2510(17). However, it is not only routinely recorded cell site data that is requested here, but rather precise location information that the government wishes to have generated in real time, at its request any time, for as long as 30 days.

Id. at *38 (emphasis added).

The GPS data in *Maynard* provided coordinates of the suspect's vehicle for the government to collect and analyze. Here, by contrast, the historical cell site location records provided to the government by the Defendants' cellular providers only reveal which cellular towers were used to route a particular call. By extension, this information can only reveal the general vicinity in which a cellular phone is used. *See, e.g.*, Gov. Surreply, Exs. 1 & 2, ECF No. 55 (sample of actual data produced by Sprint/Nextel, Inc. reveals only the approximate location (within multiple city blocks) of the Defendants' cellular phones); *United States v. Suarez-Blanca*, No. 07-023-MHS/AJB, 2008 WL 4200156, at *10-11 (N.D. Ga. Apr. 21, 2008) (discussing the imprecise nature of historical cell site location data).

Moreover, the government in *Maynard* physically installed a GPS tracking device on the suspect's vehicle without a valid warrant, and did not seek a court order pursuant to the Stored Communications Act.[8] This distinction is also important. As will be discussed *infra*, the Stored Communications Act provides a judicial backstop by which a neutral magistrate must evaluate the government's request for historical cell site location data. While the standard of "specific and articulable facts" requires a lesser showing than does probable cause, a judicial review of the government's application is required under the Stored Communications Act—a judicial review that was not present in the *Maynard* case.

Notwithstanding these differences, the courts finding that a warrant is required for extended periods of historical cell site location data acquisition have seized on *Maynard's*

[8] This distinction is not meant to suggest that the government could have relied on the Stored Communications Act to acquire real-time GPS location data in *Maynard*. As discussed by Magistrate Judge Gauvey of this Court, precise real-time location data "is nothing like the information courts have found to fall under the purview of § 2703 [of the Stored Communications Act]." *In re Application of the United States*, __ F. Supp. 2d __, No. 10-2188-SKG, 2011 WL 3423370, at *38 (D. Md. Aug. 3, 2011); *see also supra* note 7.

reasoning, and in particular on the "mosaic" theory introduced in that case. For example, Magistrate Judge Orenstein, of the Eastern District of New York, has noted that he "relied heavily on the reasoning in *United States v. Maynard*" in concluding that there is "no material difference between the essentially real-time surveillance accomplished in *Maynard* by means of a [GPS] device and retrospective location tracking via historical [cell site location] records." *See In re Application of the United States*, No. 11-MC-0113, 2011 WL 679925, at *1 (E.D.N.Y. Feb. 6, 2011). Similarly, Judge Garaufis, of the Eastern District of New York, followed "*Maynard's* persuasive reasoning" to conclude that "cumulative cell-site location records implicate sufficiently serious protected privacy concerns . . . ." *In re Application of the United States*, 809 F. Supp. 2d 113, 118, 126 (E.D.N.Y. 2011).

The Supreme Court granted certiorari in *Maynard sub nom. United States v. Jones*, and recently issued its opinion in that case. *See infra* note 6. The Court unanimously concluded that the government's surreptitious installation of a GPS device on the defendant's car was a "search" under the Fourth Amendment, but split 5-4 over the reasoning behind that decision. The majority opinion, authored by Justice Scalia, affirmed the result, and only the result, of the D.C. Circuit's *Maynard* case and concluded that the physical act of installing a GPS device on the defendant's vehicle with the purpose of obtaining information was a trespass and a Fourth Amendment search. *See Jones*, 565 U.S. __, No. 10-1259, slip op. at 4 (January 23, 2012) (Scalia, J.) ("The government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."). The majority opinion, joined by Chief Justice Roberts, and Justices Kennedy,

Thomas, and Sotomayor, expressly declined to consider whether such a "search" violated an individual's reasonable expectation of privacy. *Id.* at 12.

Concurring in the judgment, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, wrote that the majority's approach "will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked." *Id.* at 9 (Alito, J., concurring). Justice Alito, after suggesting that Congress is in the best position to determine how much surveillance society should accept as reasonable, echoes the D.C. Circuit's *Maynard* decision in concluding that:

> Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. *See Knotts*, 460 U. S., at 281–282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant. We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.

Id. at 13 (Alito, J., concurring). Moreover, and of particular importance to the present case, Justice Alito specifically calls into question the Fourth Amendment implications of the government's use of cell site location data. Acknowledging the inherent imprecision of some cellular location records, Justice Alito notes that "[t]he availability and use of these and

other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements." *Id.* at 11 (Alito, J., concurring).

Acknowledging the "vexing problems" identified by Justice Alito, Justice Scalia wrote that although electronic surveillance without physical trespass "may be . . . an unconstitutional invasion of privacy, [ ] the present case does not require us to answer that question." *Id.* at 11 (Scalia, J.). Responding to Justice Alito, Justice Scalia writes:

> . . . There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. *See post*, at 13–14. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.

Id. at 12 (Scalia, J.).

Concurring separately, Justice Sotomayor agrees with the majority "at a minimum," *id.* at 1 (Sotomayor, J., concurring), but also apparently agrees with Justice Alito's observations, *id.* at 3. While not formally joining the Alito concurrence (which would seemingly create two separate majority opinions), Justice Sotomayor intimates that her view of a reasonable expectation of privacy is even broader than the Alito formulation. She writes:

> . . . As Justice Alito incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Post,* at 10–11. Under that rubric, I agree with Justice Alito that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Post,* at 13.
>
> . . . .
>
> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.

Id. at 3-4 (Sotomayor, J., concurring).

Accordingly, it appears as though a five justice majority is willing to accept the principle that government surveillance over time *can* implicate an individual's reasonable expectation of privacy. However, as will be discussed below, the factual differences between the GPS technology considered in the *Jones* case and the historical cell site location data in the present case lead this Court to proceed with caution in extrapolating too far from the Supreme Court's varied opinions in *Jones*. Until the Supreme Court or the United States Court of Appeals for the Fourth Circuit definitively conclude that an aggregation of surveillance records infringes a Fourth Amendment legitimate expectation of privacy, this Court must apply the facts of this case to the law as currently interpreted. With this background in mind, this Court now proceeds to analyze the particular question presented in this case: Whether the defendants' Fourth Amendment rights were violated when the government acquired historical cell site location data pursuant to an Order of a Magistrate Judge of this Court issued according to the standards of the Stored Communications Act

requiring specific and articulable facts, but not probable cause. This Court concludes that they were not.

A. THE FOURTH AMENDMENT

The Fourth Amendment to the United States Constitution provides that "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ." U.S. Const. amend. IV. In order to invoke the protections of the Fourth Amendment, a person must have a "justifiable," "reasonable," or "legitimate" expectation of privacy in the place or item searched. *See Smith v. Maryland*, 442 U.S. 735, 740 (1979). Precisely what makes an expectation of privacy "justifiable," "reasonable," or "legitimate," however, has never been clearly set forth. *See O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."); *Oliver v. United States*, 466 U.S. 170, 177 (1984) ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion not authorized by warrant."); *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476, 490 (2011) ("Supreme Court opinions studiously avoid saying what makes an expectation of privacy 'reasonable.'").

Nevertheless, the standard for evaluating whether a Fourth Amendment search has occurred, first enunciated by Justice Harlan in his concurrence in *United States v. Katz*, 389 U.S. 347, 361 (1967), is whether "the individual manifested a subjective expectation of privacy" in the place or item searched, and "society is willing to recognize that expectation as

reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). As the *Katz* majority noted, the first inquiry is whether the individual has shown that "he seeks to preserve [something] as private." *Katz*, 389 U.S. at 351. The second inquiry does not ask whether a reasonable person would expect a certain right of privacy, but instead whether "the individual's expectation, viewed objectively, is 'justifiable' under the circumstances." *United States v. Knotts*, 460 U.S. 276, 281 (citations omitted). Put another way, "[t]he concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities." *United States v. Jacobsen*, 466 U.S. 109, 122 (1984).[9]

In the recently decided *Jones* case, the Supreme Court made clear, that while the *Katz* test is not the exclusive test for evaluating whether a Fourth Amendment search occurred, cases "involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Jones*, 565 U.S. __, slip op. at 11 (Scalia, J.) (emphasis in original). In other words, because the collection of historical cell site location data does not involve a

[9] *See also Rakas v. Illinois*, 439 U.S. 128, 143-44 n.12 (1978) (Rehnquist, J.):

> Obviously, however, a "legitimate" expectation of privacy by definition means more than a subjective expectation of not being discovered. A burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as "legitimate." His presence, in the words of *Jones*, 362 U.S. at 267, 80 S.Ct., at 734, is "wrongful"; his expectation of privacy is not "one that society is prepared to recognize as 'reasonable.'" *Katz v. United States,* 389 U.S., at 361, 88 S.Ct., at 516 (Harlan, J., concurring). And it would, of course, be merely tautological to fall back on the notion that those expectations of privacy which are legitimate depend primarily on cases deciding exclusionary-rule issues in criminal cases. Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.

physical trespass to property, this Court must analyze the Fourth Amendment implications of the Stored Communication Act under the *Katz* test.

B. THE STORED COMMUNICATIONS ACT, CELL SITE LOCATION DATA, AND § 2703 ORDERS

Section 2703(c) of the Stored Communications Act addresses "[r]ecords concerning electronic communication service or remote computing service." 18 U.S.C. § 2703(c). The Act permits the government to obtain a court order to produce the historical cell site location data at issue in this case. Specifically, the statute states that "a governmental entity may 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 (not including the contents of communications) only when the governmental entity . . . obtains a court order for such disclosure under subsection (d) of this section." *Id.* § 2703(c)(1)(B). A Section 2703 order "may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d) (emphasis added).

It is well established that Section 2703(c)(1)(B) of the Stored Communications Act applies to historical cell site location data. *See, e.g.*, *In re Application of the United States*, 620 F.3d 304, 313 (3d Cir. 2010) (holding that historical cell site location information is "obtainable under at § 2703(d) order"); *In re Applications of the United States*, 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007) (historical cell site location information "clearly satisfies" the

definitional requirements of § 2703(c) and is therefore obtainable pursuant to a court order issued under § 2703(d)). Magistrate Judge Gauvey of this Court has noted that the type of data at issue in this case is the "least invasive" type of cellular location information and is "commonly sought" under § 2703. *In re Application of the United States*, __ F. Supp. 2d __, No. 10-2188-SKG, 2011 WL 3423370, at *38 (D. Md. August 3, 2011). The Defendants in this case do not challenge the Stored Communications Act's applicability to the cellular location data at issue.

As previously mentioned, the "specific and articulable facts" standard contained in the Stored Communications Act is a lesser one than probable cause. *See In re Application of the United States*, 620 F.3d at 313-15 (3d Cir. 2010). While not contesting the Stored Communications Act's constitutionality on its face, the Defendants contend that when the historical cell site location information sought is sufficiently extensive and prolonged, any order issued under the Act must be obtained pursuant to a warrant issued on a showing of probable cause.

C. THE DEFENDANTS' STANDING

The government initially contends that Defendants Graham and Jordan lack standing to challenge the acquisition of historical cell site location records under the Fourth Amendment. More specifically, the government argues that because Defendant Jordan supplied a fictitious name and address to his cellular service provider, he has demonstrated an intent to distance himself from that phone and its associated records, and therefore he can claim no legitimate expectation of privacy. *See* Gov. Supp. Br. at 2, ECF No. 70. The government also argues that because Sprint/Nextel, Inc. keeps the location data in the

ordinary course of business, neither Defendant can assert a Fourth Amendment challenge to subpoenas directed at the business records of a third party. *Id.* at 2-3.

In *United States v. Katz*, the Supreme Court held that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." 389 U.S. at 351 (internal citations omitted). In *Rakas v. Illinois*, the Court questioned "whether it serves any useful analytical purpose to consider this principle a matter of standing, distinct from the merits of a defendant's Fourth Amendment claim," and concluded that standing "is more properly subsumed under substantive Fourth Amendment doctrine." 439 U.S. 128, 138-39 (1978). Noting this principle, the government maintains that "[d]emonstrating standing under the Fourth Amendment [ ] requires a defendant to prove that he had a 'legitimate expectation of privacy' in the invaded place." Gov. Supp. Br. at 1 (citing *United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010)).

Accordingly, this Court will not consider the issue of "standing" a matter separate and distinct from the inquiry into the legitimacy of the Defendants' expectation of privacy in their historical cell site location data. While Defendant Jordan's use of fictitious subscriber information certainly presents one avenue by which this Court could reject his Fourth Amendment claim, *see United States v. Suarez-Blanca*, 2008 WL 4200156, at *6-7 (N.D. Ga. April 21, 2008), the real issue is whether the Defendants have a legitimate expectation of privacy in their location data captured by their cellular service providers, and not whether they have a legal or possessory interest in the property. *See Rakas*, 439 U.S. at 148-49 & n.17.

D. BUSINESS RECORDS AND THE THIRD-PARTY DOCTRINE

In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44 (citations omitted). Put another way, the Court has stated that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. 435, 443 (1976). While the Supreme Court has applied this third-party doctrine to a number of scenarios,[10] this Court finds its application to business records and dialed telephone numbers to be particularly instructive.

In *United States v. Miller*, the government subpoenaed a bank seeking financial records of the defendant. 425 U.S. at 435. The defendant challenged the subpoena on Fourth Amendment grounds, but the Court rejected that argument for separate but related reasons. First, the Court concluded that the documents at issue were not the defendant's "private papers." *Id.* at 440. Instead, they were the "business records of the banks" that "pertain[ed] to transactions to which the bank was itself a party." *Id.* at 440-41. Accordingly, the defendant could "assert neither ownership nor possession" over the records. *Id.* Second, the Court determined that the financial records at issue were "voluntarily conveyed to the

[10] *See, e.g.*, *Hoffa v. United States*, 385 U.S. 293, 302 (1966) (applying the third-party doctrine to confidential statements made in the presence of informant); *Lewis v. United States*, 385 U.S. 206 (1966) (same); *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (target of SEC investigation not entitled to notice of issuance of subpoenas to third parties); *Donaldson v. United States*, 400 U.S. 517, 522-23 (1971) (taxpayer not entitled to intervene in proceeding to enforce IRS summonses directed at taxpayer's former employer).

banks and exposed to their employees in the ordinary course of business," and therefore "in revealing his affairs to another," the defendant took the risk "that the information [would] be conveyed by that person to the government." *Id.* at 443.

Like the bank records at issue in *Miller*, the historical cell site location records in this case are not the "private papers" of the Defendants—instead, they are the "business records" of the cellular providers. Federal law does not mandate that cellular providers create or maintain this type of data,[11] and even courts that have concluded that government acquisition of cumulative cell site location records can violate the Fourth Amendment generally acknowledge that these records are "generated in the ordinary course of the provider's business." *In re Application of the United States*, 747 F. Supp. 2d 827, 841 (S.D. Tex. 2010) (Smith, Mag. J.), *appeal docketed*, No. 11-20554 (5th Cir. Dec. 14, 2011). Moreover, insofar as historical cell site records are created and maintained by the cellular providers, individual customers do not generally have access to those records, and could not be expected to produce them in response to a subpoena. Under the reasoning of *Miller*, therefore, historical cell site location records are the provider's business records, and are not protected by the Fourth Amendment.

---

[11] Cellular providers are required to maintain for eighteen months "the name, address, and telephone number of the caller, telephone number called, date, time and length of the call" pursuant to 47 C.F.R. § 42.6. This requirement, however, does not pertain to historical cell site location data.

However, if cellular providers *were* required to keep such records, this Court's analysis would not change. In *Miller*, the bank was required by the Bank Secrecy Act to keep the records at issue. Because the records contained "only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," the Court determined that the mandatory record keeping did not create a Fourth Amendment interest in those records "where none existed before." *Miller*, 425 U.S. at 441-42.

In *Smith v. Maryland*, the Court applied the third-party doctrine to dialed telephone numbers. At the request of police, a telephone company installed a pen register on the home of a suspect in a crime, and the information derived from that pen register was later used to obtain a search warrant. 442 U.S. at 737. In investigating anonymous and harassing telephone calls to a female victim, the police were able to determine that the calls were made from the home of the defendant. The Supreme Court concluded that the installation and use of the pen register was not a Fourth Amendment "search" under the rubric of the third-party doctrine: "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers that he dialed." *Id.* at 744.

Like the dialed telephone numbers in *Smith*, the Defendants in this case voluntarily transmitted signals to cellular towers in order for their calls to be connected. The cellular provider then created internal records of that data for its own business purposes. Interestingly, at the time *Smith* was decided, telephones were almost exclusively "land lines" that were, by necessity, tethered to a particular location. The data gleaned from toll records or pen registers, therefore, encompassed "location" data with far more precision than the historical cell site location records at issue in the present case, and typically that location would be one in which the user had a Fourth Amendment privacy interest, such as a home or office At best, the records in this case identify the closest cellular tower, whereas the pen register records at issue in *Smith* indicated the physical address of the defendant's telephone. The concept of a legitimate expectation of privacy in one's location or movement simply was

not contemplated in those early telephone cases. *See also*, *Reporters Committee for Freedom of the Press v. AT & T*, 593 F.2d 1030, 1042-46 (D.C. Cir. 1978).

Both *Miller* and *Smith* stand for the proposition that by voluntarily conveying information to a third party, a person is cognizant of, and consents to the sharing of that information by the third party.[12] Numerous courts have extended the third-party doctrine well beyond bank records and telephone numbers to, *inter alia*, credit card statements, electric utility records, motel registration records, and employment records. *See, e.g.*, *United States v. Suarez-Blanca*, 2008 WL 4200156, at *8 (N.D. Ga. April 21, 2008) (collecting cases). Many courts have explicitly applied the third-party doctrine to historical cell site location records. *See supra* pp. 8-9. Magistrate Judge Gauvey's opinion, although relevant to the issue at hand, dealt with the *prospective* gathering of GPS data.

While, the issue of *historical* cell site location records appears to be one of first impression in the Fourth Circuit, the Court recently applied the third-party doctrine to internet subscriber information, and concluded that there is no legitimate expectation of privacy in such information. *See United States v. Bynum*, 604 F.3d 161, 164 (4th Cir. 2010). In *Bynum*, the FBI, in the course of investigating a child pornography suspect (Bynum), issued an administrative subpoena on Yahoo! Inc. to ascertain the internet subscriber information used in a Yahoo chat room. *Id* at 162. Yahoo provided the information and the FBI was then able determine the internet service company that provided internet service to the

[12] Importantly, the third-party doctrine analysis employed in *Miller* and *Smith* does not extend to the *contents* of communications transmitted via third party networks—under the *Katz* test, the *contents* of communications *are* entitled to Fourth Amendment protection. *See Katz*, 389 U.S. at 352 ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

suspect. *Id.* at 162-63. Information subpoenaed from the internet service provider allowed the FBI to identify the telephone and internet companies that provided the suspect's internet access. *Id.* at 163. A third administrative subpoena to the internet company revealed Bynum's name and physical address. *Id.* Using this information, the FBI sought and obtained a search warrant for Bynum's home. Bynum moved to suppress the evidence gathered pursuant to the search warrant, in part on the ground that the evidence constituted the fruit of "unlawful administrative subpoenas." *Id.* The Fourth Circuit affirmed the district court's denial of the motion to suppress and held that "Bynum voluntarily conveyed [his subscriber information] to his internet and phone companies. In so doing, Bynum 'assumed the risk that th[os]e compan[ies] would reveal [that information] to police.'" *Id.* at 164 (quoting *Smith v. Maryland*, 442 U.S. at 744) (alterations in original).

Importantly, the "subscriber information" at issue in *Bynum* included the "physical address" of the defendant—in other words, the Fourth Circuit found no reasonable expectation of privacy in information that conveyed the precise location of the defendant's home to the authorities. *Id.* In making this determination, the court noted that "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation." *Id.* (quoting *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases)). Moreover, the "administrative subpoenas" at issue in *Bynum* were not issued pursuant to the Stored Communications Act, and therefore were only subject to a "general reasonableness" standard, *id.* at 164 n.2, unlike the Section 2703 orders in this case, which required a Magistrate Judge of this Court to determine whether the government provided "specific and

articulable facts" in support of its application. In short, the Fourth Circuit in *Bynum* concluded that because Bynum voluntarily conveyed his location to his internet company, he enjoyed no reasonable expectation of privacy in that information. *Id.* at 164; *see also In re § 2703(d) Order*, 787 F. Supp. 2d 430, 429-30 (E.D. Va. 2011) (applying *Bynum* to Stored Communications Act application, and finding no reasonable expectation of privacy in social networking service subscriber information).

Based on clear Supreme Court and Fourth Circuit precedent, this Court finds the third-party doctrine applicable to historical cell site location information. Like the bank records at issue in *Miller*, the telephone numbers dialed in *Smith*, and the subscriber information collected in *Bynum*, historical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers. As part of the ordinary course of business, cellular phone companies collect information that identifies the cellular towers through which a person's calls are routed. Some courts have concluded that a cellular customer does not "voluntarily" convey this information to his cellular provider on the ground that cellular phone users are ignorant of how a cellular phone operates. *See, e.g.*, *In re Application of the United States*, 620 F.3d 304, 317 (3d Cir. 2010) ("it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information"). However, the Supreme Court's statement in *Smith* that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through the telephone company's switching equipment that their calls are completed . . . [a]ll subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial[,]" cautions against any assumption

of ignorance on the part of cellular customers. Additionally, any assumption of ignorance is belied by Sprint/Nextel, Inc.'s privacy policy, which informs its customers that it collects location data.[13]

The Eastern District of New York, which ultimately concluded that historical cell site records *are* subject to a legitimate expectation of privacy, found "unpersuasive" the Third Circuit's finding that cellular customers are ignorant regarding the records kept by their providers. *In re Application of the United States*, 809 F. Supp. 2d 113, 121 (E.D.N.Y. 2011). More to the point, that court concluded that "[n]othing in the case law . . . supports the conclusion that any minor technical distinction between the dialing [of] a phone number and the conveyance of cell-site-location records on a cell phone is constitutionally significant." *Id.* at 122. Instead, the court determined that while the third-party doctrine would ordinarily cover historical cell site location records, an exception to the third-party doctrine exists for "cumulative" records. *Id.* Relying on the mosaic theory of the Fourth Amendment created by the D.C. Circuit in *Maynard*, the court found that "cumulative cell-site-location records implicate sufficiently serious protected privacy concerns," and that "cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records, despite the fact that those records are collected and stored by a third party." *Id.* at 126.

[13] Sprint/Nextel's Privacy Policy states, in part:

> Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, *where it is located*, what device you are using, what you have purchased with your device, how you are using it, and what sites you visit.

http://www.sprint.com/legal/privacy.html (last visited February 29, 2012) (emphasis added).

This Court respectfully finds that approach to be problematic. While this Court is cognizant of Justice Alito's statement in *Jones* that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," *Jones*, 565 U.S. __, slip op. at 13 (Alito, J., concurring), the law as it now stands simply does not contemplate a situation whereby traditional surveillance becomes a Fourth Amendment "search" only after some specified period of time—discrete acts of law enforcement are either constitutional or they are not. The majority opinion in *Jones* did not endorse the D.C. Circuit's mosaic theory, and the Fourth Circuit has made it clear that individuals do not have a legitimate expectation of privacy in information voluntarily conveyed to third parties. The fact of the matter is that in enacting the Stored Communications Act, Congress passed a law that rejects a warrant requirement for this type of information, but does require specific and articulable facts to be determined by a judicial officer.

Further, it is entirely unclear what the implications would be of an interpretation of the Fourth Amendment that protects "cumulative" data collected by law enforcement. Taken to its logical extreme, such a reading would theoretically affect entire police investigations, and not just surveillance via cell site location data. In *Jones*, Justice Alito stated that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable," but goes on to conclude that "the line was surely crossed" when that monitoring continued for four weeks. *Id.* If that is how the Fourth Amendment is to be interpreted, then the police could commit a constitutional violation by taking enough individually permissible steps, that in the aggregate, add up to a substantial amount of data being collected on a suspect—thereby

infringing his reasonable expectation of privacy. For example, 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.

Fourth Amendment scholars have identified some problematic consequences attendant to the mosaic theory of the Fourth Amendment. For example, Orin Kerr,[14] a law professor at the George Washington University Law School, has commented:

> . . . [T]he mosaic theory has the bizarre consequence of creating retroactive unconstitutionality. The *Maynard* opinion indicates that it would have been okay to monitor Jones for a short time. Let's say that would allow monitoring for a few trips over the course of one day. At the end of that one day, the first day of monitoring would be constitutional. If the prosecution wanted to admit that evidence, it would be fine. But by continuing to monitor the GPS device for more time, that first day of monitoring eventually and retroactively becomes unconstitutional. It becomes part of the mosaic, and the key point of *Maynard* is that the entire mosaic is considered one entity.
>
> This will place tremendous emphasis on defining the exact scope of the mosaic. If you're a defense attorney, you now need to argue that the monitoring of your client was part of a broader mosaic to get that part tossed out. In the *Maynard* case, the scope of the one mosaic was clear: It was the

[14] Professor Kerr has testified before Congress on related issues. *See, e.g.*, *Electronic Communication Privacy Act Reform: Hearing Before the Subcomm. On the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. (2010) (Statement of Orin Kerr, Professor, George Washington Univ. Law School). Moreover, one of Professor Kerr's articles was cited with approval in Justice Scalia's majority opinion in *Jones*, 565 U.S. __, slip op. at 4 (Scalia, J.), and in Justice Alito's concurrence, *id.* at 11, 13 (Alito, J., concurring).

> GPS evidence from the month of monitoring. But I don't know why it would have to be grouped that way. If you can group different pieces of evidence into mosaics, then you need a theory of grouping: You need a new theory to explain what parts of what surveillance are in the mosaic and what parts of what surveillance are outside the mosaic. This is a whole new type of Fourth Amendment challenge, and I don't see what principles there are that could keep it from becoming an extraordinary mess.

Orin S. Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, The Volokh Conspiracy (Aug. 6, 2010 2:46 p.m.), http://volokh.com/2010/08/06/.

This Court recognizes that extended periods of historical cell site location surveillance may appear to the average person rather obtrusive, but at the same time, this Court is guided by then-Justice Rehnquist's statement in *Rakas v. Illinois* that "a 'legitimate' expectation of privacy by definition means more than a subjective expectation of not being discovered. . . . Legitimate expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." 439 U.S. 128, 143-44, n.12 (1978).

In her concurrence in *Jones*, Justice Sotomayor appeared to agree with Justice Alito in her statement that, at least in the case of real-time GPS surveillance, she "would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Jones*, 565 U.S. __, slip op. at 4 (Sotomayor, J., concurring). She even indicated 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."

Id. at 5. However, unless and until the Supreme Court affirmatively revisits the third-party doctrine, the law is that a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979) (citing, *e.g.*, *United States v. Miller*, 425 U.S. 435, 443 (1976)).

Moreover, it is important to remember that the GPS surveillance in *Jones* was conducted without a valid warrant. In this regard, Justice Sotomayor "would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool [GPS tracking] so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power and prevent 'a too permeating police surveillance.'" *Id.* at 4 (quoting *United States v. Di Re*, 332 U.S. 581, 595 (1948)). In this case, however, the Stored Communications Act, with its attendant "specific and articulable facts" standard, provides the necessary judicial backstop against which executive overreaching is measured. Magistrate Judges Gauvey and Grimm were presented with specific and articulable facts tending to show that the historical cell site location records for Defendants Graham and Jordan were relevant and material to an ongoing criminal investigation. Accordingly, they issued the § 2703(d) orders pursuant to the Stored Communications Act. Because this Court concludes that the records at issue were business records kept in the ordinary course of business by the Defendants' cellular provider, the Defendants have no legitimate expectation of privacy in those records, and therefore, no Fourth Amendment violation occurred.

E. ELECTRONIC SURVEILLANCE, GPS TRACKING, & HISTORICAL CELL-SITE DATA

Although it need not be discussed at length, a separate line of Supreme Court cases also informs this Court's decision. In *United States v. Knotts*, 460 U.S. 276, 281 (1983), the Supreme Court held that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." The Court concluded that the use of a beeper, to track an automobile on public roads did not constitute a search. The Court found that the use of a beeper merely enhanced law enforcement's ability to track the suspect: "A police car following [the suspect] at a distance throughout his journey could have observed him." *Id.* at 285.

The following year, in *United States v. Karo*, 468 U.S. 705, 708 (1984), the Court limited its holding in *Knotts* in concluding that the use of a beeper in a private residence, which was not open to visual surveillance, was a search that necessitated a warrant. *Id.* at 715. Broadly speaking, these cases stand for the proposition that law enforcement conducts a Fourth Amendment "search" when it utilizes tracking technology that allows surveillance in locations that police could not monitor in the absence of that technology. *See id.* ("For purposes of the [Fourth] Amendment, the result is [an unconstitutional search] where, without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observations from outside the curtilage of the house.").

Here, the historical cell site location records at issue identify only the closest cellular tower to the Defendants' phones, and not the precise location of the Defendants themselves. The Defendants have not argued that the historical cell site records revealed

their movements in protected areas such as their homes. Indeed, even with an ever-denser cellular tower grid, such precision is impossible. Moreover, even if cell site records could definitively indicate that an individual is in his home, that information only reveals that a person made or received a phone call while at home—in other words, non-incriminatory information that is clearly obtainable via the constitutional pen register at issue in *Smith v. Maryland*. In this regard, the Defendants again fall back on the "cumulative" nature of the cell site records at issue in this case. However, as previously discussed, in this Court's judgment the Fourth Amendment does not contemplate constitutional police action that becomes illegal when aggregated. Accordingly, this Court concludes that the government's acquisition of historical cell site location records did not infringe the Defendants' Fourth Amendment rights.

F. EMERGING TECHNOLOGY & THE FOURTH AMENDMENT

The Supreme Court has cautioned that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *City of Ontario, California v. Quon*, 130 S. Ct. 2619, 2629 (2010). Because "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior . . . . Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises . . . ." *Id.* While a four-Justice minority[15] of the Supreme Court may be

[15] In light of Justice Sotomayor's apparent endorsement of Justice Alito's concurrence, *Jones* can be plausibly understood as having two separate majority opinions. In that case, it appears as though a five-to-four majority of the Court might, in the future, endorse and craft some version of a mosaic Fourth Amendment doctrine.

ready to adopt at least some formulation of a mosaic or aggregate theory of the Fourth Amendment (at least with respect to electronic surveillance), this Court is again guided by Justice Alito's concurring statement in *Jones* that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Jones*, 565 U.S. __, slip op. at 13 (Alito, J.). Indeed, as Magistrate Judge Gauvey of this Court exhaustively recounted, privacy concerns with respect to electronic surveillance have been vigorously debated in Congress, *see In re Application of the United States*, 2011 WL 3423370, at nn.14-16, 20 and accompanying text (detailing the congressional debate surrounding privacy in location information) and that body is likely in the best position to balance the competing interests at play. As Professor Kerr has noted:

> [T]here are sound reasons to treat developing technologies differently. These differences suggest that statutory rules rather than constitutional rules should provide the primary source of privacy protections regulating law-enforcement use of rapidly developing technologies. When technology is in flux, Fourth Amendment protections should remain relatively modest until the technology stabilizes. . . . [T]he legislative branch rather than the judiciary should create the primary investigative rules when technology is changing.

Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805-806 (2004). Accordingly, the privacy issues surrounding the collection of cumulative historical cell site location records are best left to Congress—at least until the Supreme Court definitively considers the matter. In the words of Justice Alito, "[t]he best that we can do in this case is to apply existing Fourth Amendment doctrine." *Jones*, 565 U.S. __, slip op. at 13 (Alito, J.).

II. SUPPRESSION WOULD NOT BE THE REMEDY

The government argues that even if this Court were to find that the historical cell site location records were acquired in violation of the Defendants' Fourth Amendment rights, suppression of that evidence should not be the remedy insofar as the officers involved relied in good faith on the Stored Communications Act and the Orders issued by Magistrate Judges Gauvey and Grimm. In *United States v. Leon*, 468 U.S. 897, 926 (1984), the Supreme Court held that evidence obtained by law enforcement in objective good faith reliance on a facially valid search warrant is admissible even if the search warrant is ultimately deemed invalid. In *Illinois v. Krull*, 480 U.S. 340, 349 (1987), the Court held that the exclusionary rule does not apply where officers obtain evidence in "objectively reasonable reliance on a statute."

In this case, law enforcement's reliance on the Stored Communications Act and Magistrate Judges Gauvey and Grimm's Orders was objectively reasonable. First, the Defendants' have not called into question the Stored Communications Act, and the only case that questioned its constitutionality has been vacated. *See Warshak v. United States*, 490 F.3d 455, 479-80 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008) (en banc).[16] Because the Defendants have not argued that the Stored Communications Act is, in fact, unconstitutional, this Court need not address that issue insofar as it concludes that the officers acted in good-faith reliance on, and in compliance with, the requirements of a valid statute. *See Krull*, 480 U.S. at 357 n.13. Where defendants have argued that the Stored Communications Act is unconstitutional as applied (as the Defendants so argue here), other

[16] The first *Warshak* panel questioned the constitutionality of the Stored Communications Act where the government attempted to obtain the *contents* of e-mail communications, and not historical cell site location data. 490 F.3d at 460; *see also supra* n.12.

courts have concluded that suppression is inappropriate. *See United States v. Warshak*, No. 06-CR-00111, 2007 WL 4410237, at *4-5 (S.D. Ohio Dec. 13, 2007); *United States v. Ferguson*, 508 F. Supp. 2d 7, 9-10 (D.D.C. 2007). Accordingly, this Court finds that it was objectively reasonable for law enforcement to rely on the Stored Communications Act in obtaining historical cell site location data in this case.

Additionally, it was objectively reasonable for law enforcement to rely on the Orders issued by Magistrate Judges Gauvey and Grimm. Both Magistrate Judges applied the correct standard under the Stored Communications Act and found that law enforcement offered specific and articulable facts in support of the applications. *See United States v. Suarez-Blanca*, No. 07-CR-0023-MHS/AJB, 2008 WL 4200156, at *12 (N. D. Ga. Apr. 21, 2008) (applying the *Leon* good faith analysis to orders issued under the Stored Communications Act). While the Supreme Court has recognized an exception to the *Leon* good faith doctrine where "it is obvious that no reasonably competent officer would have concluded that a warrant should issue," *Mally v. Briggs*, 475 U.S. 335, 341 (1986), the Court also recently confirmed that this is a "narrow exception" and that "the threshold for establishing this exception is a high one, and it should be." *Messerschmidt v. Millender*, 565 U.S. __, No. 10-704, slip op. at 10 (Feb. 22, 2012). Here, the Defendants have not argued that this "narrow exception" to the good faith rule applies, and this Court concludes that it does not.

Even if the government's acquisition of historical cell site location records in this case had been in violation of the Defendants' Fourth Amendment rights, it obtained those records in good faith reliance on a constitutional statute and valid Orders issued by Magistrate Judges Gauvey and Grimm of this Court.

CONCLUSION

For the reasons discussed above, the Defendants' Motion to Suppress Evidence (ECF No. 38) is DENIED.

A separate Order follows.

Dated: March 1, 2012

/s/
Richard D. Bennett
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA,	*	
V.	*	
AARON GRAHAM,	*	CRIMINAL NO.: RDB-11-0094
AND		
ERIC JORDAN	*	
DEFENDANTS	*	

* * * * * * * * * * * * *

ORDER

For the reasons stated in the foregoing Memorandum Opinion, it is this 1st day of March 2012, ORDERED that:

1. Defendants' Motion to Suppress Evidence (ECF No. 38) is DENIED; and
2. The Clerk of the Court transmit copies of this Order and accompanying Memorandum Opinion to Counsel.

/s/
Richard D. Bennett
United States District Judge