IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING DISCLOSURE OF LOCATION INFORMATION OF A SPECIFIED WIRELESS TELEPHONE

NO. 10-2188-SKG

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

2011 U.S. Dist. LEXIS 85638

August 3, 2011

Susan K. Gauvey, United States Magistrate Judge.

MEMORANDUM OPINION AND ORDER

The issue before the Court is the government's authority to prospectively acquire precise location information derived from cellular and Global Positioning System ("GPS") technology (collectively "location data") to aid in the apprehension of the subject of an arrest warrant. The government has reported no attempts of the subject to flee and the requested location data does not otherwise constitute evidence of any crime. The government argues its entitlement to prospective location data under these circumstances pursuant to the *Fourth Amendment*, *Rule 41 of the Federal Rules of Criminal Procedure*, the Stored Communications Act, the All Writs Act, and the inherent authority of the court. In so doing, the government asks to use location data in a new way -- not [*2] to collect evidence of a crime, but solely to locate a charged defendant. To some, this use would appear reasonable, even commendable and efficient. To others, this use of location data by law enforcement would appear chillingly invasive and unnecessary in the apprehension of defendants. In any event, there is no precedent for use of location data solely to apprehend a defendant in the absence of evidence of flight to avoid prosecution. The government did not submit, and the court did not find, any sufficient authority for this use of location technology. In light of legitimate privacy concerns and the absence of any emergency or extraordinary considerations here, the Court concludes that approval of use of location data for this purpose is best considered deliberately in the legislature, or in the appellate courts. Accordingly, the Court DENIES the underlying warrant applications, but sets forth its guidance on the showing necessary for law enforcement access to prospective location data to aid in the execution of an arrest warrant.

I. BACKGROUND

A. Procedural History

On June 3, 2010, pursuant to *Federal Rule of Criminal Procedure 41* ("*Rule 41*") and the Stored Communications Act, *18 U.S.C. ß 2703(c)(1)(A)*, [*3] the United States ("government") applied for "authoriz[ation]...to ascertain the physical location of the [subject] cellular phone..., including but not limited to E911 Phase II data (or other precise location information)...for a period of thirty (30) days." (ECF No. 1, ∂ 2). The government also asked for "records reflecting the tower and antenna face ("cell site") used by the target phone at start and end of any call" where precise location information was not available. (Id. at n.1). The government asked that the Court order the wireless service provider to send a signal to defendant's cell phone ("ping") that would direct the phone to compute its current GPS coordinates and communicate that data back to the provider, which would in turn forward the coordinates immediately to government agents. (Id. at ∂ 16). The government based its request on "probable cause to believe that the Requested Information w[ould] lead to evidence regarding certain activities described above." (Id. at ∂ 12). The government has asked that the particulars of the application not be disclosed, but has stipulated that defendant's location was not evidence of a crime. The government also stated that the "requested [*4] information [was] necessary to determine the location of [the subject] so that law enforcement officers may execute the arrest warrant [on him]." (Id.). The Court denied the government's application.

On June 4, 2010, the government submitted another application seeking identical information as its first application, but further stated that the subject cell phone was pre-equipped with a GPS enabled chip and that the subject's wireless service provider maintains a "Precision Locate Service" [1] capable of approximating the location of any telephone so equipped. (ECF No. 2, ∂ 2). The government explained that, in order to use the Precision Locate Service, the cellular service provider "sends a signal to a telephone directing it to immediately transmit its current GPS reading, then processes the reading to compute the telephone's current GPS Coordinates." (Id.). The government elaborated that the Precision Locate Service can be used "without disclosing to a telephone's user the existence of either the Carrier's signal requesting the telephone to send a current GPS reading or that telephone's response." (Id.). The government asked for an order directing the wireless service provider "on oral [*5] request . . . at any times specified by the agents [to] use its Precision Locate Service . . . to acquire the GPS Coordinates." (ECF No. 2, 7).

1 The service to which the government refers in its application is actually called "Sprint Precision Locator."

Although the government in its first application invoked *Rule 41* and the Stored Communications Act, the government's second application cited as authority the All Writs Act, *28 U.S.C. ß 1651(a)*. (Id. at ∂ 4). Specifically, the government noted:

> The Court has authority pursuant to the All Writs Act, *28 U.S.C. ß 1651*, to order disclosure of GPS Coordinates on a showing of **probable cause to believe that a federal fugitive is using a specified wireless telephone.** Under *28 U.S.C. ß 1651(a)*, such disclosure is of appropriate aid to the Court's extant jurisdiction over an open arrest warrant because it assists agents to find the fugitive so that the warrant can be executed and he can be brought before the Court.

(Id.) (emphasis added). In support of its application, the government stated that:

> On [XXXX], Special Agent [XXXX] of [XXX] called [defendant] on cellular telephone number [XXX-XXX-XXXX], which he answered and indicated he was on the "west [*6] coast." She asked if he was in [XXXX] and he said, "Yes." [Defendant] had previously given this cellular telephone number to SA [XXXX] as a means to contact him.

(Id.). The government referred to defendant as a "federal fugitive" and "the subject fugitive," but alleged no facts to support defendant's fugitive status. (Id.). There was no indication that defendant was aware of the charge or arrest warrant, and the government did not so allege. (ECF No. 15, 17-18). Other than the government's applications under review here, there were no reported efforts on the part of law enforcement to apprehend and arrest the defendant. See (ECF No. 6, 1). The Court again denied the government's application.

Notwithstanding the Court's denial of location data, the government arrested the defendant a few days thereafter. (Id.). While the government is correct that apprehension of defendant moots its applications, the issues presented will certainly arise again, most likely in urgent situations that do not allow an opportunity for deliberate consideration. Because of the importance of these largely-unexplored issues, the Court writes this opinion. Although the government's applications have been sealed, [*7] this opinion will not be sealed as it concerns matters of constitutional and statutory interpretation which do not hinge on the particulars of the underlying investigation and charge. The issues explored herein involve the balance between privacy rights and law enforcement interests, and the role of judicial oversight. These particular issues present a matter of first impression in the Fourth Circuit, as well as many others. [2]

> 2 After denying the government's applications, the Court invited further argument and authorities from the government, appointed the Office of the Federal Public Defender to provide the defense perspective, and held a hearing. (ECF Nos. 4, 5, 7, 11, 12). The Court thanks the Office of the United States Attorney, the U.S. Department of Justice, and the Office of the Federal Public Defender for their briefing and argument.

B. Technological Background

At the outset, a basic review of GPS and cellular location technology is essential to understanding the nature of the government's request -- highly-precise, real-time GPS and cell-site location information, on demand at any time during a 30-day period and the privacy interests it implicates. Given that the Court did not [*8] take evidence on the relevant technology, this background discussion relies primarily on uncontroverted government and industry publications. [3] Moreover, there is no dispute as to two key technical points, namely the minimum precision of the location data requested (within 300 meters or less) (ECF No. 15, 22) and the fact that the GPS data requested is not collected as part of the routine provision of cellular telephone service (Id. at 26-31).

> 3 For a comprehensive finding of facts regarding the technology used in cellular location tracking, see *In re Application of the United States . . ., 747 F. Supp. 2d at 831-835 (S.D. Tex. 2010)*.

The government's request for "E911 Phase II data" is a reference to location information that meets accuracy requirements mandated by the Federal Communication Commission's Enhanced 9-

1-1 ("E-911") regulations, which require cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls. E-911 Phase II regulations mandate that cellular telephone carriers have the ability to provide, within six minutes of a valid request from a public safety answering point, the latitude [*9] and longitude of a cellular telephone caller to within 50 to 300 meters depending on the type of technology used. See *47 C.F.R. 20.18(h) (2011)* (establishing accuracy and reliability standards of 100 meters for 67 percent of calls and 300 meters for 95 percent of calls for network-based (non-GPS) technologies, and 50 meters for 67 percent of calls and 150 meters for 95 percent of calls for handset-based (GPS) technologies). The government at the hearing conceded that, due to the requirements of the E-911 regulations, its request would necessarily locate the subject cellular telephone within 300 meters. (ECF No. 15, 22). As set forth below, however, current GPS technology would almost certainly enable law enforcement to locate the subject cellular telephone with a significantly greater degree of accuracy -- possibly within ten meters or less.

The Global Positioning System or "GPS" is a space-based radionavigation utility owned and operated by the United States that provides highly-accurate positioning, navigation, and timing services worldwide to any device equipped with a GPS satellite receiver. See GPS.GOV, THE GLOBAL POSITIONING SYSTEM, http://www.gps.gov/systems/gps/ (last visited [*10] Jul. 5, 2011). To determine the location of a cellular telephone using GPS, special hardware in the user's handset calculates the longitude and latitude of the cellular telephone in real time based upon the relative strength of signals from multiple satellites. ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 20, 21 (2010) (statement of Matt Blaze, Associate Professor, University of Pennsylvania) ("Blaze Testimony").

Current GPS technology typically achieves spatial resolution within ten meters, or approximately 33 feet. Id. at 21; see also The Collection and Use of Location Information for Commercial Purposes: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection and Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce, 111th Cong. 4 (2010) (statement of John B. Morris, General Counsel and Director of CDT's Internet Standards, Technology & Policy Project, Center for Democracy and Technology) (stating that GPS produces high-precision locations on the order of meters or tens [*11] of meters). High-quality GPS receivers, however, are capable of achieving horizontal accuracy of 3 meters or better and vertical accuracy of 5 meters or better 95 percent of the time. U.S. DEPT. OF DEFENSE, GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE PERFORMANCE STANDARD v (4th ed. Sept. 2008). Use of GPS in combination with augmentation systems enables real-time positioning within a few centimeters. See GPS.GOV, AUGMENTATION SYSTEMS, http://www.gps.gov/systems/augmentations/ (last visited Apr. 21, 2011) (explaining that a GPS augmentation is any system that aids GPS by providing accuracy, integrity, availability, or any other improvement to positioning, navigation, and timing that is not inherently part of GPS itself).

Despite the superior accuracy of GPS location technology, however, it is not without limitations. Cellular telephone users may be able to disable GPS functionality and GPS may not work reliably in the event that the receiver's view of satellites is obstructed. Blaze Testimony at 22; see also ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. [*12] Comm. on the Judiciary, 111th Cong. 41 (2010) (statement of Michael Amarosa, Senior Vice President for

Public Affairs, TruePosition) ("GPS devices can be deactivated - that is, the ability to locate them disabled -- by the user").

In the event that GPS location data is not available, the government's request also sought access to cell-site location data. See (ECF No. 1, n.1) (requesting access to "records reflecting the tower and antenna face ("cell site") used by the target phone at the start and end of any call"). While GPS location technology locates a user by triangulating satellite signals, "cellular identification locates a user by triangulating their position based on the cell towers within signal range of their mobile phone." The Collection and Use of Location Information for Commercial Purposes: Hearing Before the Subcomm. on Commerce, Trade and Consumer Protection and Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy and Commerce, 111th Cong. 3 (2010) (statement of Lori Faith Cranor, Professor of Computer Science and of Engineering & Public Policy, Carnegie Mellon University). Cellular providers can obtain cell-site location information even [*13] when no call is in progress. Id. This data is routinely collected and tracked by cellular service providers, at various time intervals depending on the provider. Blaze Testimony at 23; See also CTIA-The Wireless Association, Wireless Glossary of Terms, http://www.ctia.org/media/industry_info/index.cfm/AID/10321 (last visited Jul. 28, 2011) (explaining that each "registration," or cell phone-initiated contact with a cell tower, is automatically logged by the cell and stored temporarily by the phone's unique Electronic Serial Number (ESN)). While retention practices vary by carrier, many retain registration data only for about 10 minutes, unless the cell phone has registered again at the same or another cell tower. See FTC Workshop, "Introduction to Privacy and Security Issues Panel" (Dec. 12, 2000), available at http://www.ftc.gov/bcp/workshops/wireless/001212.htm. However, when a user makes a call, the carrier records the cell tower that originated that call, and this information is retained, and often appears on the user's bill. Id. Unlike GPS, network-based location technology cannot be affirmatively disabled by the user. Blaze Testimony at 22.

Due to advances in technology and the [*14] proliferation of cellular infrastructure, cell-site location data can place a particular cellular telephone within a range approaching the accuracy of GPS. Id. at 23-27 (explaining that depending upon a variety of factors the accuracy of cell-site location data may range from miles in diameter to individual floors and rooms within buildings); see also *In re Application of the United States. . ., 747 F. Supp. 2d 827, 834 (S.D. Tex. Oct. 29, 2010)* ("As cellular network technology evolves, the traditional distinction between "high accuracy" GPS tracking and "low accuracy" cell site tracking is increasingly obsolete, and will soon be effectively meaningless."). Cellular service providers can also employ a hybrid method or combination of methods to locate phones with considerable precision even where GPS or cell-site technology alone would be inadequate. One example of many hybrid location techniques currently in use is Assisted GPS (A-GPS), an enhanced version of GPS that uses advanced techniques and hardware to allow reception of GPS signals indoors. FED. COMMUNIC'NS COMM'N., FCC REPORT TO CONGRESS ON THE DEPLOYMENT OF E-911 PHASE II SERVICES BY TIER III SERVICE PROVIDERS, [*15] 7 n.29 (2005).

Cellular service providers typically do not maintain records of the GPS coordinates of cellular telephones operating on their network, but the provider may generate such location data at any time by sending a signal directing the built-in satellite receiver in a particular cellular telephone to calculate its location and transmit the location data back to the service provider. This process, known as "pinging," is undetectable to the cellular telephone user. In the underlying applications, the government seeks an order directing Sprint Nextel to "ping" the subject cellular telephone and

use its Precision Locator ServiceSM to provide the resulting location data to the government. See GPSREVIEW.NET, SPRINT OFFERS GPS FLEETING TRACKING THROUGH PRECISION LOCATOR WIRELESS DEVICES (Aug. 24, 2005), http://www.gpsreview.net/sprint-offers-gps-fleet-tracking-through-precision-locator-wireless-devices/ (last visited Apr. 21, 2011) (describing the Precision Locator Service[SM] as an interactive location and mapping application marketed to businesses as a way to communicate with and monitor a mobile and decentralized staff). To use the Precision Locator Service[SM], subscribers or other [*16] authorized parties log onto a website hosted by Sprint to locate and track a particular cellular telephone in real time [4], to map or export its location information, and to determine whether GPS-capabilities are powered on or off. Id. The government noted in its application that, "the Carrier has advised that the [sic] Precision Locate Service can be used unobtrusively, i.e., without disclosing to a telephone user the existence either of the Carrier's signal requesting the telephone to send a current GPS reading or that telephone's response." (ECF No. 2, ∂ 2).

> 4 "Real time" in this context is a term of art. "Prospective" location data includes any location information generated after the date of the court order permitting the government to obtain that information. See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 81-85 (2010) (statement of The Honorable Stephen Wm. Smith, United States Magistrate Judge, Southern District of Texas). "Real-time" location data is a subset of prospective location data which includes only information [*17] that is both generated after the court's order and is provided to the government in, or close to, "real time." Id. (explaining that prospective and real-time location data are distinguishable from "historical" location data, which encompasses only that location information that already has been created, collected, and recorded by the cellular service provider at the time the court authorizes a request for that information). The government's request for GPS and cell-site location information encompasses both prospective and real-time location data.

Here, the government seeks more than the records generated in the ordinary course of provision of cellular service, i.e., the cell site used by a target phone at the beginning and end of a call and the cell site detected at routine, intermittent registration. Rather, the government requested an order requiring the carrier "at any times specified by the agents" to acquire the GPS coordinates of the subject cellular telephone, thus asking for the creation of a record that would not otherwise be generated in the ordinary provision of service. Moreover, the government asked for an order for a period not to exceed 30 days, which would allow essentially [*18] continuous monitoring of the precise location of the user for a month. Thus, the issue is whether the request for highly-accurate, prospective and real-time location data of the cell phone of a non-fugitive defendant for as long as 30 days on an essentially continuous basis is permissible under the *Fourth Amendment*, *Rule 41*, the Stored Communications Act, the All Writs Act, or the inherent authority of the Court.

II. ANALYSIS

A. Government's Arguments and Defense Response

The government bases its entitlement to prospective location data under the *Fourth Amendment* on essentially two, alternative arguments. First, the government argues that the underlying arrest

warrant provides the necessary authority for access to the location data under the *Fourth Amendment* and interpretive Supreme Court decisions, particularly *Payton v. New York, 445 U.S. 573, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980)*. The government apparently posits that the existence of the arrest warrant supplants or satisfies the probable cause requirement of a search warrant as defined by *Fourth Amendment* jurisprudence. Alternatively, the government argues that *Warden v. Hayden, 387 U.S. 294, 87 S. Ct. 1642, 18 L. Ed. 2d 782 (1976)*, permits the use of a search warrant to obtain evidence in aid of [*19] apprehension of a defendant, such as the location data at issue here, even where there is no evidence of flight, that is, where the location data would not be evidence of a crime.

Having taken the stance that its request does not offend, and indeed is consistent with, the *Fourth Amendment*, the government presents various statutory grounds for access to this prospective location data. In its first application, the government argues that the requested warrant is authorized under *Rule 41* and the Stored Communications Act. In its second application, the government, apparently recognizing the absence of clear statutory authority, argues that issuance of a search warrant for prospective location data under the circumstances presented is proper under the Court's inherent power and the All Writs Act.

The Federal Public Defender argues that an arrest warrant does not authorize access to location data for the subject of the arrest warrant and that the *Fourth Amendment* prohibits use of a search warrant to access prospective location data where the information does not constitute evidence of a crime. Thus, the argument goes, governmental assertions of authority under the Stored Communications Act, [*20] *Rule 41*, the All Writs Act, or the Court's inherent authority are futile, as the warrant does not comport with the *Fourth Amendment*.

This case presents an issue at the intersection of the law on arrests and searches: whether this "search" should be considered under the second clause of the *Fourth Amendment* (the "warrant" clause) or as a "reasonable" search in execution of an arrest warrant under the first clause of the *Fourth Amendment* - an exception to the procedures and requirements of the warrant clause. This case also reveals the dearth of analysis and authority on this issue. The Court has concluded that current *Fourth Amendment* jurisprudence neither sanctions access to location data on the basis of an arrest warrant alone, nor authorizes use of a search warrant to obtain information to aid in the apprehension of the subject of an arrest warrant where there is no evidence of flight to avoid prosecution and the requested information does not otherwise constitute evidence of a crime. Additionally, the Stored Communications Act (also, of course, subject to the *Fourth Amendment*) does not authorize use of a warrant for that purpose. While *Rule 41(c)(4)* authorizes use of a warrant to [*21] search for a "person to be arrested," that rule (and *Fourth Amendment* principles) requires probable cause that the defendant will be found in a specifically identified location. *Fed. R. Crim. P. 41(c)(4)*. Thus, *Rule 41* does not authorize use of a warrant for the purpose sought. Finally, exercise of judicial authority under the All Writs Act or the Court's inherent authority is likewise subject to *Fourth Amendment* constraints. Review of pertinent case law demonstrates that the courts have not sanctioned use of a warrant or other order for location data or other extraordinary information to aid in the apprehension of the subject of a warrant in the absence of evidence of flight.

This ruling does not, of course, foreclose use of a search warrant to obtain prospective location data in circumstances where the *Fourth Amendment* is satisfied. While the Court disagrees that the Stored Communications Act provides independent authority for access to prospective location data under these circumstances, the Court finds that the government may obtain prospective location

data where that data constitutes evidence of a crime under the *Fourth Amendment*. Had the government's request included demonstration [*22] of the fugitive status of the subject of the arrest warrant, the request would have been fairly routine. Courts grant warrants for location data where presented with facts demonstrating flight to avoid prosecution, most frequently in conjunction with a complaint charging this new, criminal violation against a defendant already charged with a serious crime. See *18 U.S.C. ß 1073 (2011)*.

However, if the government seeks to use a particular cellular telephone as a tracking device to aid in execution of an arrest warrant, the government must obtain a tracking device warrant pursuant to *Rule 41(b)* and in accord with *18 U.S.C. ß 3117*. As set forth more fully below, this Court requires a showing of probable cause that: 1) a valid arrest warrant has issued for the user of the subject cellular telephone; 2) the subject cellular telephone is in the possession of the subject of the arrest warrant; and 3) the subject of the arrest warrant is a fugitive, that is, is or could be charged with violation of *18 U.S.C. ß 1073*. Moreover, the time period of the warrant must be measured by its purpose, that is, only until the defendant is located, to prevent inappropriate use of the warrant as an investigative [*23] tool.

Having summarized its conclusions, the Court discusses each of the government's asserted bases for entitlement in turn.

B. Asserted Sources of the Government's Entitlement to Location Data

1. *Fourth Amendment*

a. Protected Status of Information Sought Under the *Fourth Amendment*

The government and Federal Public Defender agree that this matter is at heart a question of *Fourth Amendment* interpretation. (ECF No. 8, 1-2; ECF No. 10, 2). Specifically, the *Fourth Amendment* 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, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV. Rooted in early British constitutionalism and the American colonial experience of unchecked monarchic power, the *Fourth Amendment* protects individual privacy by establishing a right to be secure against unreasonable searches and seizures by the government. See *Chimel v. California, 395 U.S 752, 760-61, 89 S. Ct. 2034, 23 L. Ed. 2d 685 (1969)* (citing *United States v. Rabinowitz, 339 U.S. 56, 69, 70 S. Ct. 430, 94 L. Ed. 653 (1950)* [*24] (Frankfurter, J., dissenting)). Accordingly, the threshold issue in every *Fourth Amendment* analysis is whether a particular government action constitutes a "search" or "seizure" within the meaning of the Amendment. See *United States v. Jacobsen, 466 U.S. 109, 113, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984)* (stating that the *Fourth Amendment* "protects two types of expectations, one involving 'searches,' the other 'seizures.'"); see also Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment ß2.1 (2010) (explaining that the words "searches and seizures" are terms of limitation; law enforcement practices do not fall within the ambit of the *Fourth Amendment* unless

they are either "searches" or "seizures."). Historically, courts resolved this inquiry using a property trespass theory. See *Olmstead v. United States, 277 U.S. 438, 457, 48 S. Ct. 564, 72 L. Ed. 944 (1928)*. More recently, the Supreme Court has moved beyond this paradigm to broaden the range of privacy interests protected under the *Fourth Amendment*. See, *Katz v. United States, 389 U.S. 347, 353, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)*.

In Katz v. United States, the Court famously noted that the *Fourth Amendment* "protects people, not places," *389 U.S. 347, 351, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)*, and developed an analytical framework under [*25] which the Amendment's protection of privacy interests is implicated wherever there is a "reasonable expectation of privacy," *id. at 360-61* (Harlan, J. concurring). The modern test for analyzing the expectation question is two-part: first, whether the defendant has exhibited an actual, subjective, expectation of privacy; and second, whether such subjective expectation is one which society is willing to recognize as objectively reasonable. Id.; see, *California v. Greenwood, 486 U.S. 35, 40-41, 108 S. Ct. 1625, 100 L. Ed. 2d 30 (1988)*; *United States v. Karo, 468 U.S. 705, 715, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984)*.

b. An Individual Has a Reasonable Expectation of Privacy in His Location and Movement

The government's request for real-time location data implicates at least two distinct privacy interests: the subject's right to privacy in his location and his right to privacy in his movement. [5]

> 5 Some courts and commentators have suggested that prolonged surveillance might also implicate the subject's *First Amendment* rights of freedom of association. See e.g., Vivek Kothari, Autobots, Decepticons, and Panopticons: The Transformative Nature of GPS Technology and the Fourth Amendment, *6 Crim. L. Brief 37, 45 (2010)* ("More than mere locations, GPS devices provide [*26] an index of known associates and associations and insight into the frequency of those associations. The attachment of a GPS device, then, implicates fundamental *First Amendment* freedom of association concerns."). Notably, The Supreme Court has emphasized that the *Fourth Amendment* warrant requirement should be "scrupulously observed" when *First Amendment* concerns are presented. See *Stanford v. Texas, 379 U.S. 476, 484-85, 85 S. Ct. 506, 13 L. Ed. 2d 431 (1965)* (noting in the context of a warrant for seizure of books that "unrestricted power of search and seizure could also be an instrument for stifling liberty of expression"). However, this opinion does not analyze this potentially, additional bases for the privacy right.

The government conceded at the hearing that the subject has a reasonable expectation of privacy while physically present within a non-public place, and that the government would infringe upon that privacy interest by asking the wireless carrier to "ping" the subject's cell phone essentially on a continuous basis while he is in a constitutionally-protected location. [6] (ECF No. 15, 4). At the same time, the government suggested, but could not satisfactorily support, that the subject of an arrest warrant [*27] has a diminished expectation of privacy in his location. (ECF No. 15, 5) (It is "less clear that someone [who is the subject of an arrest warrant] has an expectation of privacy in their location."). The Court finds that the subject here has a reasonable expectation of privacy both in his location as revealed by real-time location data and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days.

> 6 While the government does not make the argument here that the subject of the arrest warrant relinquished his expectation of privacy in his location information by voluntarily

sharing it with a third party, it has invoked this argument in a number of other cases. See e.g., *In re Application of the United States for an Order . . ., 620 F.3d 304, 317 (3d. Cir. 2010)* ("The Government argues that no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider."); *In re the Application of the United States for an Order . . ., 534 F. Supp. 2d 585, 613-614 (W.D. Pa. 2008)* ("The Government has contended, and some Courts have opined, that there is no reasonable [*28] expectation of privacy in CSLI because cell-phone-derived movement/location information is analogous to the dialed telephone numbers found unprotected by the Supreme Court in Smith v. Maryland."); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F.Supp. 2d 747, 756-57 (S.D. Tex. 2005)* ("The government contends that probable cause should never be required for cell phone tracking because there is no reasonable expectation of privacy in call site location data, analogizing such information to the telephone numbers found unprotected in *Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)*"); *In the Matter of the Application of . . ., 402 F.Supp. 2d 597, 605 (D. Md. 2005)* ("The government claims a warrant is never required because cell site information does not implicate the *Fourth Amendment*, even when the possessor resides in a private place. The government reaches this conclusion by analogizing cell site information to dialed telephone numbers, See *Smith v. Maryland, 442 U.S. 735, 742-44, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)* (dialed telephone numbers do not implicate the *Fourth Amendment*)"). In making this argument, the government has relied upon the Supreme Court's holding in *Smith, 442 U.S. at 742-45*, [*29] that telephone users have no reasonable expectation of privacy in phone numbers dialed or other necessary routing-type information generated during a phone call because they voluntarily expose such information to a third party, the service provider.

It is relevant to the instant matter, however, that several courts have distinguished the unprotected telephone numbers in Smith from cell site location data. See *United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004)*; *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F.Supp. 2d 747, 756-57 (2005)*(discussing Forest and stating that "[u]nlike dialed telephone numbers, cell site data is not voluntarily conveyed by the user to the phone company. It is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge.")(internal quotations omitted); *In the Matter of An Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 736 F.Supp.2d 578, 582-584 (E.D.N.Y. Aug. 27, 2010)*(finding that Smith does not apply to cell-site location data and that recent cases undermine the government's [*30] reliance on Smith to suggest that a reasonable expectation of privacy disappears when information is held by a third-party service provider). Critically, the Third Circuit in a recent cell site decision stated that "[A] cell phone customer has not shared his location information with a cellular provider in any meaningful way...it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information." *In re Application of the United States for an Order . . ., 620 F.3d at 317*. This finding is particularly significant given the ubiquity of cellular telephones in modern American society. See Aaron Smith, Pew Internet & American Life Project, Mobile Access 2010, 12 (Jul. 7, 2010) available at http://pewinternet.org/~/media//Files/Reports/2010/PIP_Mobile_Ac cess_2010.pdf (reporting that 82 percent of adults own a cell phone.)

Finally, here the government seeks information - essentially, continuous pinging - that is not collected as a necessary part of cellular phone service, nor generated by the customer in placing or receiving a call. Under this circumstance it is difficult to understand how the user "voluntarily" exposed such information [*31] to a third party.

i. An Individual Has a Reasonable Expectation of Privacy in His Location

The Supreme Court has maintained a distinction between areas where a person can be publicly viewed and areas that could not be observed "from the outside" using traditional investigatory techniques. For example, a person has no reasonable expectation of privacy in his movements on public highways during a discrete journey. *United States v. Knotts, 460 U.S. 276, 281, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983)*. Because traditional, visual surveillance allows the government to observe a person's movements in public areas, the fact that the government chooses to do so electronically does "not alter the situation." Id. However, the government does run afoul of the *Fourth Amendment* when it uses enhanced surveillance techniques not available to the public to "see" into private areas. *Kyllo v. United States, 533 U.S. 27, 34, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)* (holding that warrantless use of a thermal imaging device that allowed surveillance into a private home violated the *Fourth Amendment* because it allowed the government to "obtain[] by sense-enhancing technology [] information regarding the interior of the home that could not otherwise have been obtained without [*32] a physical 'intrusion into a constitutionally protected area'"); *United States v. Karo, 468 U.S. 705, 715, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984)*.

While location data has been described as "a proxy for [the suspect's] physical location" because the cell phone provides similar information as that traditionally generated by physical surveillance or tracking techniques, *United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004)*, abrogated by *United States v. Booker, 543 U.S. 220, 125 S. Ct. 738, 160 L. Ed. 2d 621 (2005)* (on other grounds), that is not entirely correct. Location data from a cell phone is distinguishable from traditional physical surveillance because it enables law enforcement to locate a person entirely divorced from all visual observation. Indeed, this is ostensibly the very characteristic that makes obtaining location data a desirable method of locating the subject of an arrest warrant. This also means, however, that there is no way to know before receipt of location data whether the phone is physically located in a constitutionally-protected place. In other words, it is impossible for law enforcement agents to determine prior to obtaining real-time location data whether doing so infringes upon the subject's reasonable expectation of [*33] privacy and therefore constitutes a *Fourth Amendment* search. However, the precision of GPS and cell site location technology considered in combination with other factors demonstrates that pinging a particular cellular telephone will in many instances place the user within a home, or even a particular room of a home, and thus, the requested location data falls squarely within the protected precinct of *United States v. Karo, 468 U.S. 705, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984)* and *United States v. Kyllo, 533 U.S. 27, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)*. Consider, for instance, the import of the following.

Coordinates expressed in longitude and latitude allow us to locate places on the Earth quite precisely -- to within inches. NATIONALATLAS.GOV, ARTICLE: LATITUDE AND LONGITUDE, http://www.nationalatlas.gov/articles/mapping/a_latlong.html (last visited Jul. 19, 2011). GPS technology typically generates location data accurate within a range of approximately ten meters, Blaze Testimony at 21, or within a few centimeters when used in combination with augmentation systems, GPS.GOV, AUGMENTATION SYSTEMS, http://www.gps.gov/systems/augmentations/ (last visited Jul. 19, 2011). Thus, location data generated by GPS and expressed as longitude and latitude

coordinates [*34] will identify a point on a map that, in many cases, represents the location of a particular GPS-enabled cellular telephone within a radius of ten meters or significantly less.

Given that the average home size in the United States in 2009 was approximately 743 square meters, it is clear that GPS location data with the high degree of accuracy described above would likely place a cellular telephone inside a residence, at least where law enforcement have information regarding the coordinates of the home. U.S. CENSUS BUREAU, MEDIAN AND AVERAGE SQUARE FEET OF FLOOR AREA IN NEW SINGLE-FAMILY HOUSES COMPARED BY LOCATION, available at http://www.census.gov/const/C25Ann/sftotalmedavgsqft.pdf (statistics include houses built for rent). Such information about the coordinates of various physical structures would almost certainly be available to law enforcement. For example, publicly-available interactive mapping programs such as Google Earth display satellite images of the Earth's surface, allowing users to view the latitude and longitude of physical structures. See GOOGLE EARTH, ABOUT GOOGLE EARTH: WHAT IS GOOGLE EARTH?, http://earth.google.com/support/bin/answer.py?hl=en&answer=17614 5 (last visited [*35] Jul. 19, 2011). In addition, the U.S. Census Bureau began using handheld computers in 2010 to collect the GPS coordinates of every residence in the United States and Puerto Rico as part of its address canvassing efforts. U.S. CENSUS BUREAU, ADDRESS CANVASSING FACTS/STATISTICS, available at http://2010.census.gov/news/press-kits/one-year-out/address-canvasing/address-canvassing-facts-statistics.html.

Because cellular telephone users tend to keep their phone on their person or very close by, placing a particular cellular telephone within a home is essentially the corollary of locating the user within the home. See PEW RESEARCH CENTER, CELL PHONES AND AMERICAN ADULTS, available at http://pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults.aspx (reporting that 65 percent of adults with cell phones report sleeping with their cell phone on or right next to their bed). In addition, cell phone users typically carry their phone on their person when conducting daily activities. See *In re United States for an Order . . ., 534 F. Supp. 2d 585, 597 (W.D. Pa. 2008)* ("Our individual cell phones now come with us everywhere: not only on the streets, but in (a) a business, financial, medical, [*36] or other offices; (b) restaurants, theaters, and other venues of leisure activity; (c) churches, synagogues, and other places of religious affiliation; and (d) the homes of our family members, friends, and personal and professional associates.").

The Court recognizes that a determination that, based on GPS location data, a cellular telephone user is within a particular physical place may require some inference, but notes the Supreme Court's admonition in Kyllo v. United States that "the novel proposition that inference insulates a search is blatantly contrary to *United States v. Karo, 468 U.S. 705, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984)*, where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home. The police activity was held to be a search, and the search was held unlawful." *533 U.S. 27, 36-37, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)*. Indeed, as the Court of Appeals for the Third Circuit recently noted, "the Government has asserted in other cases that a jury should rely on the accuracy of [] cell tower records to infer that an individual, or at least her cell phone, was at home." *In re Application of the United States for an Order. . ., 620 F.3d 304, 311-12 (3d. Cir. 2010)* (citing Brief for Electronic Frontier [*37] Foundation, et al. as Amici Curiae Supporting Affirmance of the District Court, *In re Application of the United States . . ., 620 F.3d 304 (3d. Cir. 2010))*. Of course, the location information derived from cell tower records is considered less precise than the GPS data at issue here.

Thus, as the majority of other courts that have examined this issue have found, the *Fourth Amendment* requires that the government must show probable cause prior to accessing such data. See, e.g., *In re the Application of the United States . . ., 396 F. Supp. 2d 294, 323 (E.D.N.Y. 2005)*("Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate *Fourth Amendment* privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking . . . which routinely require probable cause."); *In re the Application of the United States . . ., 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006)* ("[D]etailed location information, such as triangulation and GPS data, [] unquestionably implicate *Fourth Amendment* privacy rights."); *In re Application the of the United States . . ., 402 F. Supp. 2d 597, 604-05 (D. Md. 2005)* (recognizing that monitoring [*38] of cell phone location information is likely to violate a reasonable expectation of privacy).

ii. An Individual Has a Reasonable Expectation of Privacy in His Movements

The scope of the government's request here - unlimited location data at any time on demand during a thirty-day period - also implicates the subject's reasonable expectation of privacy in his movement. See *United States v. Maynard, 615 F.3d 544, 562, 392 U.S. App. D.C. 291 (D.C. Cir. 2010)* (holding that "the whole of a person's movements over the course of a month is not actually exposed to the public" and is therefore protected by the *Fourth Amendment*). See also *U.S. v. Bailey, 628 F.2d 938, 949 (6th Cir. 1980)* (holding that "privacy of movement itself is deserving of *Fourth Amendment* protections"); *United States v. Moore, 562 F.2d 106, 110 (1st Cir. 1977)* (agreeing that "citizens have a reasonable expectation of privacy in their movements, and that the possibility of being followed about in public by governmental agents does not mean that they anticipate that their every movement will be continuously monitored by a secret transmitter").

While Knotts held that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation [*39] of privacy in his movements from one place to another," *460 U.S. at 281*, it expressly reserved the issue of 24-hour surveillance, *id. at 283-84*. Addressing this issue, the United States Court of Appeals for the District of Columbia held that "prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble." *Maynard, 615 F.3d at 562*. [7] But cf. *United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010)* (holding that GPS tracking of defendant's car did not invade defendant's reasonable expectation of privacy and did not constitute a *Fourth Amendment* search because it revealed only information the agents could have obtained by physically following the car). Although the Ninth Circuit denied rehearing en banc in Pineda-Moreno, five judges dissented from the denial by published opinion. United States v. Pineda-Moreno, reh'g en banc denied, *617 F.3d 1120 (9th Cir. 2010)*. In the lead dissent, Chief Judge Alex Kozinski argued that GPS tracking is much more invasive than the use of beepers discussed in Knotts, which merely augmented visual surveillance actually being conducted [*40] by the police; the combination of GPS tracking with other technologies in common use by law enforcement amounts to a virtual dragnet in dire need of regulation by the courts; and such "creepy and un-American" behavior should be checked by the *Fourth Amendment*. *Id. at 1126* (Kozinski, C.J., dissenting from the denial of reh'g en banc).

7 A few short months after the District of Columbia Circuit's decision in Maynard, the United States Court of Appeals for the Third Circuit considered government access to historical cell site data for the first time and, while not ultimately resolving the *Fourth*

Amendment issue, concluded that the factual record was insufficient to determine whether historical cell site records could encroach upon a citizens' reasonable expectations of privacy regarding their physical movements and locations. *In re Application of the United States . . ., 620 F.3d 304 (3d. Cir. 2010)*. The Third Circuit opined, "We cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which [*41] provides information as to the actual whereabouts of the subject." *Id. at 312*.

Several district courts have since declined to adopt the D.C. Circuit's reasoning in Maynard. See *United States v. Sparks, 750 F. Supp. 2d 384, 391-392 (D. Mass. 2010)* (finding that warrantless installation and monitoring of a GPS device attached to defendant's vehicle did not violate the *Fourth Amendment* where law enforcement did not invade any constitutionally-protected area within defendant's dwelling or curtilage to attach the device, and used it to locate the vehicle only on public streets and highways); *United States v. Walker, No. 10-32, 2011 U.S. Dist. LEXIS 13760, at *20 (W.D. Mich. Feb. 11, 2011)* (warrantless installation and use of a GPS device to track a vehicle as part of a drug trafficking investigation did not violate the *Fourth Amendment* where defendant's vehicle was parked in a public lot when police attached the device and there was no evidence that law enforcement used the device to monitor defendant's location anywhere other than on public thoroughfares). These cases are distinguishable from the instant matter, however, because they clearly deal with movement in a largely, if not entirely, [*42] public setting, that is, vehicle tracking. Here, of course, the tracking is of a cell phone, which is ordinarily on a person. While a vehicle may as a matter of fact remain within public spaces during a tracking period (not go into a private garage or other private property), it is highly unlikely - indeed almost unimaginable - that a cell phone would remain within public spaces.

Given that a person has a reasonable expectation of privacy in his aggregate movement over a prolonged period of time, the government's request to ping the subject's cell phone on unlimited occasions during a thirty-day period constitutes a *Fourth Amendment* search.

Having established that the defendant has a reasonable expectation of privacy in his location and his movement, the Court considers the government's argument that a search warrant for real-time location data is not necessary, as a matter of law, where an arrest warrant based upon probable cause has issued.

c. The Subject of an Arrest Warrant Maintains a Reasonable Expectation of Privacy in His Location and Movements

The government contends that where a valid arrest warrant has been issued for the cell phone user, government officials are entitled to [*43] "do what it takes to find and arrest the person." (ECF No. 15, 8). [8] Specifically, the government asserts that the arrest warrant authorizes acquisition of location data, even without further court warrant or order. "[T]he warrant for the arrest of the subject itself gives law enforcement sufficient authority to obtain location information for his phone without a further search warrant." (ECF No. 6, 8).

8 At the hearing, the government also suggested that it was "less clear that someone [who is the subject of an arrest warrant] has an expectation of privacy in their location."). (ECF No. 15, 5). However, the government had no authority for its proposition that the subject of an

arrest warrant enjoyed less of an expectation of privacy, than an uncharged person. (Id.). Apparently, this position is based solely on *Payton v. New York, 445 U.S. 573, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980)*.

> The notion that the subject of an arrest warrant relinquishes any reasonable expectation of privacy in his "person, houses, papers, and effects" upon a neutral magistrate's determination of probable cause that he has committed a crime -- a concept that is implicit in the government's argument even if not explicitly stated -- is clearly inconsistent [*44] with existing constitutional limitations on law enforcement. Even where law enforcement officers may permissibly enter a suspect's residence without a search warrant in order to execute an arrest warrant under Payton, their authority to search the residence is limited to recognized exceptions to the *Fourth Amendment* search warrant requirement. For instance, officers may search areas of the home where the subject might reasonably be hiding in order to locate him (i.e., they may search a closet, but not a shoe box). In the interest of safety, officers may also conduct a protective sweep of the home, *Maryland v. Buie, 494 U.S. 325, 110 S. Ct. 1093, 108 L. Ed. 2d 276 (1990)*(holding that the *Fourth Amendment* permits a properly limited protective sweep in conjunction with an in-home arrest when the searching officer possesses a reasonable belief based on specific and articulable facts that the area to be swept harbors an individual posing a danger to those on the arrest scene), and may search the area within the arrestee's immediate control, *Chimel v. California, 395 U.S. 752, 89 S. Ct. 2034, 23 L. Ed. 2d 685 (1969)*(holding that, absent a search warrant, an arresting officer may search only the area "within the immediate control" of the person arrested, meaning [*45] the area from which he might gain possession of a weapon or destructible evidence). These recognized exceptions to the search warrant requirement are grounded in concerns about safety and exigency, rather than an expansive view of the authority inherent in an arrest warrant.

For support, the government relies upon the Supreme Court's decision in *Payton v. New York, 445 U.S. 573, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980)*, and an unreported Southern District of Indiana case, United States v. Bermudez, IP-05-43-CR, 2006 WL 3197181 (S.D. Ind. Jun. 30, 2006). (ECF No. 10, 7); (ECF No. 15, 6) ("If we [the government] hold the ability to [ping defendant's phone] without involving any third party, I think Payton establishes that it is okay."). The government notes that Payton establishes inter alia that it is constitutionally reasonable to require the subject of an arrest warrant to "open his doors" to law enforcement officers seeking to execute the warrant. See (ECF No. 15, 9-10). On this basis, the government concludes that its possession of a valid arrest warrant in this case authorizes the "lesser" infringement of accessing location information pertaining to the suspect. Id. The government reasons that,

> Going into the home [*46] is one of the most protected areas in the *Fourth Amendment* -- . . . And yet in Payton, the Supreme Court says an arrest warrant is good enough to go into the target's home.
>
> I think it follows that other lesser interests are also going to be subject or appropriate under an arrest warrant for the Government to get the information it needs to effectuate the arrest warrant.

Id.

Payton and its progeny may be read as affording less procedural protection to the privacy rights of an un-apprehended defendant in his location - that is, that law enforcement is not required to obtain prospective judicial approval through a search warrant. However, the case law does not clearly establish that there is a lesser burden than demonstration of reasonable belief that the defendant is in the premises as a prerequisite for entry. Moreover, Payton does not support the government's bold declaration that the arrest warrant authorizes law enforcement "to do what it takes to find and arrest the person and determine the location of the person." (ECF No. 15, 8). To state the obvious: the arrest warrant demonstrates probable cause to arrest a person; the arrest warrant does not demonstrate probable cause that the [*47] person is in any particular place. Payton cannot be read to absolve the government from having a reasonable belief that the suspect is in a particular location before it may enter to effectuate an arrest warrant. Finally, the Court does not agree with the government's characterization of access to location data as necessarily a lesser infringement of privacy than Payton's limited access to a person's home, in the wired and watched era of the 21st century.

In Payton, the Supreme Court held that a routine felony arrest made during a warrantless and nonconsensual entry into a suspect's home violates the *Fourth Amendment*. *445 U.S. 573, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1982)*. In addition, the Payton Court announced, ". . . for *Fourth Amendment* purposes, an arrest warrant founded on probable cause implicitly carries with it the limited authority to enter a dwelling in which the suspect lives when there is reason to believe the suspect is within." *Id. at 602-03* (emphasis added). The Court concluded that a search warrant was unnecessary (or would be redundant) under these circumstances. The Court reasoned that, "[i]f there is sufficient evidence of a citizen's participation in a felony to persuade a judicial officer that his [*48] arrest is justified, it is constitutionally reasonable to require him to open his doors to the officers of the law." Id. [9]

> 9 Although the arrest warrant in Payton was for a felony, courts have held that Payton authorizes entry into a suspect's residence to effectuate a valid misdemeanor arrest warrant. See *Smith v. Tolley, 960 F.Supp. 977, 991 (E.D. Va. 1997)*("[I]t is irrelevant whether the underlying offense for which the arrest warrant is secured is a felony or misdemeanor."); *United States v. Spencer, 684 F.2d 220, 223 (2nd Cir. 1982)*, cert. denied *459 U.S. 1109, 103 S. Ct. 738, 74 L. Ed. 2d 960 (1983)*; *United States v. Gooch, 506 F.3d 1156, 1158-59 (9th Cir. 2007)*, cert. denied *552 U.S. 1331, 128 S. Ct. 1922, 170 L. Ed. 2d 782 (2008)*. Regardless of the precise nature of the underlying charge, however, courts demand that law enforcement must have a "reasonable belief" that the suspect lives at the place to be entered and is present there. *Ward v. Moore 414 F.3d 968, 971 (8th Cir. 2005)*("A valid arrest warrant, whether for a felony or misdemeanor, carries with it the authority to conduct a forcible entry so long as the police have a reasonable belief that the suspect resides at the place to be entered and is currently present there.").

Thus, Payton does [*49] not deny that an entry into the home of the subject of an arrest warrant is a "search" (or an invasion of a reasonable expectation of privacy), but merely concludes that it is a constitutionally reasonable one. However, this narrow exception to the *Fourth Amendment* search warrant requirement does not negate the subject's expectation of privacy in his own home, much less in any other location. Rather than granting police unlimited authority to enter a suspect's home when armed with a valid arrest warrant, as would presumably be appropriate if the arrest warrant deprived the suspect of any reasonable expectation of privacy, the Payton Court mandated that

police have a "reasonable belief" that the suspect both lives at the place to be searched and is present within the place to be searched at the time of arrest. *Id. at 602-03*. Thus, it is clear that an arrest warrant alone does not justify entry of a residence to apprehend the subject of the warrant. See *United States v. Gorman, 314 F.3d 1105 (9th Cir. 2002)* ("An arrest warrant forms only the necessary, rather than sufficient, basis for entry into a home, and, in addition to an arrest warrant, there must be reason to believe the suspect [*50] is within the residence.").

One year after its decision in Payton, the Supreme Court delineated additional limitations on law enforcement's authority in execution of an arrest warrant in *Steagald v. United States, 451 U.S. 204, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981)*. In Steagald, police entered the home of the defendant to apprehend a third-person who was the subject of an arrest warrant. *Id. at 205*. At trial, the defendant sought to suppress the evidence against him on the grounds that the police officers did not possess a search warrant when they entered his home. *Id. at 205-07 (1981)*. Addressing the narrow, unresolved issue of "whether an arrest warrant - as opposed to a search warrant - is adequate to protect the *Fourth Amendment* interests of persons not named in the warrant when their homes are searched without their consent and in the absence of exigent circumstances," *id. at 212*, the Steagald Court held that the *Fourth Amendment* does not permit police to enter a third person's home to serve an arrest warrant on a suspect. *Id. at 205-06*. The Court determined that an arrest warrant does not sufficiently protect the *Fourth Amendment* rights of parties not named in the warrant. *Id. at 212-13*. Based upon this reasoning, [*51] the Court held that law enforcement must obtain a search warrant before entering a third-party residence to apprehend the subject of an arrest warrant. *Id. at 205-06*.

Although Steagald focused on the privacy interests of third-party residents rather than persons for whom an arrest warrant has issued, the Court made clear that an arrest warrant does not give law enforcement officers authority to enter any dwelling where they believe a suspect may be found. The Steagald Court recognized that "[a] contrary conclusion -- that the police, acting alone and in the absence of exigent circumstances, may decide when there is sufficient justification for searching the home of a third party for the subject of an arrest warrant -- would create a significant potential for abuse." *Id. at 215*. The Court also expressed concern that an arrest warrant "may serve as a pretext for entering a home in which police have suspicion, but not probable cause to believe, that illegal activity is taking place." Id. In other words, the Steagald Court declined to find that an arrest warrant represents an exception to the search warrant requirement of probable cause allowing law enforcement unfettered authority to pursue [*52] the subject of an arrest warrant.

Finally, the Supreme Court in Steagald did not share the government's view of the expansive meaning of Payton. The Supreme Court in Steagald characterized its ruling in Payton as "authoriz[ing] a limited invasion of that person's privacy interest when it is necessary to arrest him in his home." *Id. at 214* (emphasis added). Thus Payton and Steagald are scant authority for the government's bold assertion that the arrest warrant here allows the sweeping invasion of the defendant's privacy rights -- 24/7 tracking of his movements for as long as 30 days to effect the arrest -- without any demonstration of necessity such as fugitive status.

In addition to Steagald, the Supreme Court has cited Payton 78 times since rendering its decision in 1980. None of these cases involves a remotely similar fact situation as here and none expand the Payton holding as a doctrinal matter. The government can point to no subsequent, supportive Supreme Court decision but clings to its view of the Payton concept of plenary authority to effect an arrest warrant. Significantly, the Supreme Court has cited Payton most frequently not as an exception to the warrant clause in the arrest [*53] situation, but as standing for the cardinal

principle that absent consent or exigent circumstances, law enforcement may not enter a private home to effectuate an arrest without a warrant. See, e.g., *Brigham City v. Stuart, 547 U.S. 398, 403, 126 S. Ct. 1943, 164 L. Ed. 2d 650 (2006)*; *Georgia v. Randolph, 547 U.S. 103, 109, 126 S. Ct. 1515, 164 L. Ed. 2d 208 (2006)*; *Groh v. Ramirez, 540 U.S. 551, 559, 124 S. Ct. 1284, 157 L. Ed. 2d 1068 (2004)*; *Kaupp v. Texas, 538 U.S. 626, 630, 123 S. Ct. 1843, 155 L. Ed. 2d 814 (2003)*; *Kirk v. Louisiana, 536 U.S. 635, 635-636, 122 S. Ct. 2458, 153 L. Ed. 2d 599 (2002)*; *Kyllo v. United States, 533 U.S. 27, 31, 40, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001)*. [10]

10 The Supreme Court also has cited Payton as support for general *Fourth Amendment* concepts on a number of occasions. See, e.g., *Illinois v. McArthur, 531 U.S. 326, 331, 121 S. Ct. 946, 148 L. Ed. 2d 838 (2001)* (citing *Payton, 445 U.S. at 591*, for the proposition that "[t]he chief evil against which the *Fourth Amendment* is directed is warrantless entry of the home[,]"); *City of Ladue v. Gilleo, 512 U.S. 43, 58, 114 S. Ct. 2038, 129 L. Ed. 2d 36 (1994)* (citing *Payton, 445 U.S. at 590*, for the proposition that "[a] special respect for individual liberty in the home has long been part of our culture and our law").

The Supreme Court has cited Payton only occasionally for the proposition that an arrest warrant provides authority to infringe upon the expectation of the privacy of the [*54] subject in his home or elsewhere, and, in none of those cases can be viewed as a significant expansion of Payton. See, e.g., *Maryland v. Buie, 494 U.S. 325, 330, 110 S. Ct. 1093, 108 L. Ed. 2d 276 (1990)*("It is not disputed that until the point of Buie's arrest the police had the right, based on the authority of the arrest warrant, to search anywhere in the house that Buie might have been found, including the basement.") (emphasis added); *Pembaur v. City of Cincinnati, 475 U.S. 469, 488, 106 S. Ct. 1292, 89 L. Ed. 2d 452 (1986)* (Powell, J., dissenting) (noting that "In *Payton v. New York, 445 U.S. 573, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980)*, the Court rejected the suggestion that a separate search warrant was required before police could execute an arrest warrant by entering the home of the subject of the warrant.); *Michigan v. Summers, 452 U.S. 692, 704, 101 S. Ct. 2587, 69 L. Ed. 2d 340 (1981)* (same); *Steagald v. United States, 451 U.S. 204, 221, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981)* (same). None of these citations even suggest the radical expansion of government authority urged here.

Finally, several cases clearly demonstrate the Supreme Court's reluctance to approve police conduct unnecessary to the execution of an arrest warrant. See *Wilson v. Layne, 526 U.S. 603, 119 S. Ct. 1692, 143 L. Ed. 2d 818 (1999)*; *Arizona v. Hicks, 480 U.S. 321, 107 S. Ct. 1149, 94 L. Ed. 2d 347 (1987)*; *Maryland v. Garrison, 480 U.S. 79, 107 S. Ct. 1013, 94 L. Ed. 2d 72 (1987)*.

In [*55] Wilson v. Layne, the Court found that media presence during the execution of an arrest warrant in a private home violated the *Fourth Amendment*. *526 U.S. 603, 606-608, 119 S. Ct. 1692, 143 L. Ed. 2d 818 (1999)*. While the government argued that the Payton Court's finding that homeowners are required to open their "doors to officers of the law" seeking to effectuate an arrest warrant authorized the conduct in question, Brief for Respondents at 12 *Wilson v. Layne, 526 U.S. 603, 119 S. Ct. 1692, 143 L. Ed. 2d 818 (1999)* (quoting *Payton, 445 U.S. at 602-603*), the Court rejected this argument, finding media presence unrelated to the purposes of the warrant. The Court signaled judicial vigilance against an unnecessarily broad view of police arrest authority under Payton -- even in the face of purported law enforcement benefits: "[w]ere such generalized 'law enforcement objectives' themselves sufficient to trump the *Fourth Amendment*, the protections guaranteed by that Amendment's text would be significantly watered down." *Id. at 612*. [11] See also, *Arizona v. Hicks , 480 U.S. 321, 324-325, 107 S. Ct. 1149, 94 L. Ed. 2d 347 (1987)* (explaining that

the *Fourth Amendment* requires police action undertaken in execution of a warrant must relate to the objectives of the authorized intrusion); *Maryland v. Garrison, 480 U.S. 79, 86-87, 107 S. Ct. 1013, 94 L. Ed. 2d 72 (1987)* [*56] (observing that the purposes justifying a warrant "strictly limit" the manner in which the warrant is executed).

> 11 In applying Wilson, federal circuit courts have noted that *Fourth Amendment* privacy rights do not turn solely on the special status of the home. See, e.g., *Lauro v. Charles, 219 F.3d 202, 211 (2d Cir. 2000)* (citing *Katz v. United States, 389 U.S. 347, 351, 88 S. Ct. 507, 19 L. Ed. 2d 576, (1967)* ("[T]he *Fourth Amendment* protects people, not places.")). The Fourth Circuit has added that Wilson requires courts to conduct case-by-case inquiries into whether the police action undertaken in execution of a warrant is related to the "objectives of the authorized intrusion." *Hunsberger v. Wood, 583 F.3d 219, 221-222 (4th Cir. 2009)*(Wilkinson, J., concurring in the denial of reh'g en banc).

Since the Supreme Court's decisions in Payton and Steagald, five courts of appeals, not including the Court of Appeals for the Fourth Circuit, have concluded that law enforcement officers do not need a search warrant to effectuate an arrest in a third-party residence where they have a valid arrest warrant coupled with a reasonable belief that the suspect is inside. See *United States v. Jackson, 576 F.3d 465 (7th Cir. 2009)*; *United States v. Agnew, 407 F.3d 193 (3d Cir. 2005)*; [*57] *United States v. Kaylor, 877 F.2d 658 (8th Cir. 1989)*; *United States v. Buckner, 717 F.2d 297 (6th Cir. 1983)*; *United States v. Underwood, 717 F.2d 482 (9th Cir. 1983)*. Notably, these decisions do not require prior judicial approval for entrance by the government; ex-post justification is sufficient if a defendant challenges the search or seizure. Although this rule appears to contradict the rule articulated by the Supreme Court in Steagald, the apparent inconsistency can be explained by the posture of the cases --all involving the rights of the subjects of the arrest warrant, not third parties. Distinguishably, each of the defendants in the courts of appeals cases cited supra were suspects named in a valid arrest warrant, but apprehended without a search warrant in the residence of a third party. As the Sixth Circuit explained when discussing this factual scenario in United States v. Buckner, "the Payton rule does not directly apply because the defendant was not arrested in his own home" and "Steagald is also not on point because the person prosecuted in this case was the person named in the arrest warrant." *717 F.2d 297, 299 (6th Cir. 1983)*. Despite this observation, however, the Buckner [*58] Court ultimately determined that, "[t]he fact that the defendant was the person named in the arrest warrant mandates application of Payton rather than Steagald." *Id. at 300*. Other courts of appeals have similarly applied Payton when considering *Fourth Amendment* challenges made by defendants named in arrest warrants, but apprehended in the residence of a third party without a search warrant. Accordingly, these courts have found that no search warrant was constitutionally required; the arrest warrant was sufficient to protect the *Fourth Amendment* rights of the suspect, so long as there was reasonable belief that he was there. See *United States v. Jackson, 576 F.3d 465, 467-68 (7th Cir. 2009)*(under the *Fourth Amendment*, police were not required to have a search warrant as well as an arrest warrant in order to enter the apartment of an acquaintance of defendant to arrest defendant, where they had reason to suspect that defendant was inside); *United States v. Agnew, 407 F.3d 193 (3d Cir. 2005)*("[E]ven if Agnew was a non-resident with a privacy interest, the *Fourth Amendment* would not protect him from arrest by police armed with an arrest warrant."); *United States v. Kaylor, 877 F.2d 658, 663 (8th Cir. 1989)*(the [*59] possession of a warrant for the defendant's arrest and the officers' reasonable belief of his presence in a third party's home justified entry without a search warrant); *United States v. Underwood, 717 F.2d 482, 484 (9th Cir. 1983)*("If an arrest warrant and reason to believe the person named in the

warrant is sufficient to protect that person's *fourth amendment* rights in his own home, they necessarily suffice to protect his privacy rights in the home of another. The right of a third party not named in the arrest warrant to the privacy of his home may not be invaded without a search warrant. But this right is personal to the home owner and cannot be asserted vicariously by the person named in the arrest warrant.").

These cases advance the notion that the subject of an arrest warrant has lesser procedural rights, that is, a search warrant need not be obtained on probable cause prior to entry, whether to his own home or to that of a third party. Steagald and subsequent case law also advance the notion that even where law enforcement officers apprehend the subject of an arrest warrant in a third-party residence without first obtaining a search warrant, "a suspect retains a sufficient expectation [*60] of privacy to challenge a search where the police lack a reasonable belief that the person to be arrested may be found in the place to be searched." *United States v. Jackson, 576 F.3d 465, 468 n.1 (7th Cir. 2009)*(citing *United States v. Boyd, 180 F.3d 967, 977-78 (8th Cir. 1999)*; *Valdez v. McPheters, 172 F.3d 1220, 1225-26 (10th Cir. 1999)*; *United States v. Edmonds, 52 F.3d 1236, 1247-48 (3d Cir. 1995))*; see also *United States v. Cantrell, 530 F.3d 684, 689-90 (8th Cir. 2008)*; 6 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment ß 11.3 (2008)(asserting that, if the arrestee himself lacks standing to challenge an illegal search, then this would "render the Steagald rule a virtual nullity"). While Payton *Fourth Amendment* analysis arguably supports the view that the subject of an arrest warrant is accorded lesser procedural protection in his location than third parties, post-Payton case law still demands that there be reasonable belief that the subject of an arrest warrant is in a particular place to be searched. Thus, the substantive privacy right of the subject of the arrest warrant is undiminished. [12] Accordingly, case development since Payton affirms that no prior [*61] judicial approval in the form of a search warrant is necessary for entry into a defendant's home or premises of third parties where law enforcement has a reasonable belief that the defendant is there. However, nothing in post-Payton jurisprudence undermines the requirement that a search - whether based on the authority of an arrest warrant or a separately obtained search warrant - be supported by reasonable belief that the subject of the search is in a particular place. Thus, this jurisprudence does not illuminate the issue here: whether the arrest warrant alone authorizes a search for location data for the subject of an arrest warrant. While such a search does not implicate the privacy rights of third parties, and thus Payton, not Steagald, would apply, the government's request here is still without firm foundation. Payton involved permission to go into a specifically defined place; it did not address the nature of what is sought here - permission to find and track a subject of an arrest warrant wherever he is. On first blush, it may seem reasonable to obtain location data under the authority of an arrest warrant for the sole purpose of apprehending the subject of that warrant. However, [*62] the government has provided no doctrinal bridge from the "limited authority" granted to it under Payton, to the much broader and different power it seeks in this case, which is to obtain essentially continuous location and movement data pertaining to a subject of an arrest warrant over a thirty day period. Even if the Court were to limit the time period of the warrant to 30 days or a reasonable period of time after location of the cell phone and its user to allow a safe arrest, whichever is shorter, that would not address the fact that a tracking warrant provides different and arguably more information than a traditional place-based warrant would. While the government in this case has declared that its acquisition of location data represents a lesser infringement of privacy than the entry into the home permitted by Payton, the government has failed to support that proposition with either rigorous intellectual argument or legal precedent.

12 "[T]he 'reason to believe' standard was not defined in Payton, and since Payton, neither the Supreme Court, nor the courts of appeal have provided much illumination." Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment ß 6.1 (4th [*63] ed. 2004) (citing *United States v. Magluta, 44 F.3d 1530 (11th Cir. 1995)*. There is no Fourth Circuit precedent on this issue and the circuits which have examined it are split. Several courts of appeal have held that reasonable belief is synonymous with probable cause. See *United States v. Hardin, 539 F.3d 404, 416 n.6 (6th Cir. 2008)*; *United States v. Barrera, 464 F.3d 496, 501 (5th Cir. 2006)*; *United States v. Gorman, 314 F.3d 1105, 1111 (9th Cir. 2002)*; *Magluta, 44 F.3d 1530, 1535 (11th Cir. 1995)*. Others have concluded that reasonable belief represents a lesser degree of knowledge than probable cause. See *United States v. Thomas, 429 F.3d 282, 286, 368 U.S. App. D.C. 285 (D.C. Cir. 2005)*; *Valdez v. McPheters, 172 F.3d 1220, 1227 n.5 (10th Cir. 1999)*; *United States v. Lauter, 57 F.3d 212, 215 (2d Cir. 1995)*.

The constitutionality of a search under either the authority of an arrest warrant under Payton, or a search warrant under *Fourth Amendment* jurisprudence, is predicated on a probable cause demonstration that the subject of the arrest is in a particular place. While the government has adopted the reasonable belief or probable cause standard, that is, that there is "probable cause to believe that a federal [*64] fugitive is using a specified wireless telephone," (ECF No. 2, 3), it has not asked the Court for authority to go into a particular place. Instead, the government essentially seeks to "look" with technology into every place where the subject of the warrant might be found in order to locate him and then to track him up to 30 days.

The fact that a person is in his or her home at any particular time would usually not be especially revelatory. While the fact of a person's location at random times in other locations might be highly revelatory of private matters, location data over a prolonged period of time has the potential of revealing intimate details of a person's life. As Chief Judge Kozinski observed in his dissent from the denial of rehearing en banc in Pineda-Moreno,

> By tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions. It can also learn a great deal about us because where we go says much about who we are. Are Winston and Julia's cell phones together near a hotel a bit too often? Was Syme's OnStar near an STD clinic? Were Jones, Aaronson and Rutherford at that protest outside the White House? [*65] The FBI need no longer deploy agents to infiltrate groups it considers subversive; it can figure out where the groups hold meetings and ask the phone company for a list of cell phones near those locations.

Pineda-Moreno, 617 F.3d at 1125 (Kozinski, C.J., dissenting from the denial of reh'g en banc).

What difference, if any, is there, in terms of a citizen's rights to privacy against his government, between a warrant allowing the search of a particular place for the subject of an arrest warrant and allowing the search of everywhere to locate the particular place where the subject of a search warrant is? If the order is narrowly drawn and faithfully executed, there would arguably be no greater intrusion of third parties' privacy than a search of the suspect's home or other locations under Payton and its progeny, in the furtherance of the legitimate government interest in expeditiously bringing a charged defendant before the Court. An order for location data at one point in time does not appear to invade the privacy of others any more than a search warrant for a third party's home.

That is, execution of a traditional search warrant may invade the privacy of persons living in or present [*66] at the searched premises at the time of the search. However, a search warrant for location data may invade the privacy of persons not as readily identifiable as persons in a traditional search in the suspect's home, such as persons on the lease of the apartment or employees working at an office where the subject has been located.

By contrast, the search sought here does arguably infringe upon the privacy rights of the subject of the arrest warrant more than a Payton search would and certainly does provide more information. A Payton search informs the government as to whether the subject of the arrest warrant is in his home or in another place that the government had probable cause to believe he is. However, the search anticipated here informs the government on an almost continuous basis where the subject is, at places where the government lacked probable cause to believe he was, and with persons about whom the government may have no knowledge.

A warrant such as the government requested here only superficially bears the indicia of the colonial writs, which were the impetus for the *Fourth Amendment*. The *Fourth Amendment* was a reaction in part to the colonial experience with primarily two [*67] English writs: the general writ of assistance and the general warrant. "[It] was primarily designed to end the abuse of general exploratory searches. PHILLIP A. HUBBART, MAKING SENSE OF SEARCH AND SEIZURE LAW: A *FOURTH AMENDMENT* HANDBOOK, 21-49 (2005). The general writ of assistance "granted the named customs official general exploratory search powers based on no proof of wrongdoing." Id. at 30. Similarly, the general warrant "was not based on any sworn proof of wrongdoing, did not particularly describe the place to be searched or things [or people] to be seized, and authorized the messengers to search and seize as their whims dictated." Id. at 40. "The general objectionable feature of both warrants [general warrant and writ of assistance] was that they provided no judicial check on the determination of the executing officials that the evidence justified an intrusion in any particular home." *Steagald, 451 U.S. at 220.*

The odious nature of these writs, of course, was due in main part to the disruption and intrusiveness of searches unjustified by any probable cause as to a particular place as to innocent citizens. By comparison, this virtual search of all locations to identify the actual [*68] location of the arrest warrant subject does not affect the privacy of third parties, any differently than a traditional search warrant. It may affect more, or different, third parties than a traditional search, however. But, law enforcement does not physically enter and disrupt all homes - only those places where the location data indicates an arrest warrant subject's presence and only on further warrant or under exigent circumstances if in a non-public place. Of course, the virtual search does not impact those persons at locations "searched" which do not reveal his presence. On the other hand, the government's acquisition of location data on an essentially continuous basis might be seen as a kind of general "exploratory rummaging in a person's belongings" prohibited by the *Fourth Amendment*. See *Coolidge v. New Hampshire, 403 U.S. 443, 467, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971)* (plurality).

Certainly, the Supreme Court's approval of a "limited" intrusion into the home of a subject of an arrest warrant (and lower courts' approval of intrusion into third party residences on probable cause or reasonable belief) without a prior warrant cannot reasonably be interpreted to endorse other infringements of privacy, that is, [*69] the constitutional right to location and movement privacy. The government's arguments, if credited, would allow law enforcement to obtain location data on

any subject of an arrest warrant, whether charged with a misdemeanor or a felony, without any demonstration of any attempt on the part of the subject to avoid prosecution.

Ultimately, the Supreme Court may expand Payton and endorse a variant of the government's view, that is, that armed with an arrest warrant, law enforcement can take certain reasonable actions to execute the arrest warrant, such as access to location data for a short period of time, without obtaining a search warrant subject only to challenge after the fact. Indeed, this judge has concluded that it is likely that the Supreme Court would sanction this search under Payton, but perhaps with prior judicial approval in light of the powerful nature of the electronic surveillance tool. However, it is premature - indeed reckless - to forecast and effect such an expansion of law enforcement authority given the evolving nature and complexity of both *Fourth Amendment* law and technology.

This judge will not take that leap in the absence of any direct precedent or sufficient doctrinal [*70] foundation, especially in the face of considerable legislative and public concern and discussion about the invasion of privacy that this new and evolving location technology permits. Congress has repeatedly expressed concern about the privacy of location data. When Congress passed the Wireless Communication and Public Safety Act of 1999, inter alia, for the purpose of facilitating nationwide deployment of the enhanced 9-1-1 technology the government seeks to use in its investigation, the legislature expressly provided for privacy of customer information. See P.L. No. 106-81(2), ß 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at *47 U.S.C. ß 222*) (stating that "[t]he purpose of [the Wireless Safety Act of 1999] is to encourage and facilitate the prompt deployment throughout the United States of a seamless, ubiquitous, and reliable end-to-end infrastructure for communications, including wireless communications, to meet the Nation's public safety and other communications needs"). In doing so, Congress specifically included protection for the privacy of location information pertaining to cell phone users:

> (f) Authority to Use Location Information. For purposes of subsection (c)(1) of this [*71] section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to --
>
> > (1) Call location information concerning the user of the commercial mobile service...

47 U.S.C. ß 222(f). Accord *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F.Supp. 2d 747, 756-57 (2005)*. (The Court interpreted *section 222(f)* to indicate that "...location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer."). Id.

Earlier, in 1994 when Congress passed the "Communications Assistance for Law Enforcement Act" ("CALEA"), it declared that orders for pen register and trap and trace devices shall not include "any information that may disclose the physical location of the subscriber. . ." *47 U.S.C. ß 1002(a)(2)(B)*.

Indeed, Sprint Nextel -- the cellular service provider for the subject of the government's applications here -- provides in its standard privacy policy that, although it routinely collects

personal information pertaining to customers, including the location of their devices [*72] on the network, it only shares this information with third parties under certain limited circumstances. SPRINT, SPRINT NEXTEL PRIVACY POLICY,

http://www.sprint.com/legal/privacy.html (last visited Feb. 1, 2011). [13]

13 In the Consumer Resources section of its official website, Sprint Nextel further emphasizes the sensitive nature of location information in its 'Consumer Privacy FAQs'. SPRINT, CONSUMER RESOURCES -- CUSTOMER PRIVACY FAQS, http://newsroom.sprint.com/article_display.cfm?article_id=1472#q ID9 (last visited Feb. 1, 2011). In response to the frequently asked question "How is my device location information used?," Sprint Nextel states that,

> To make wireless communications possible, wireless networks use the location of your device to deliver mobile services whenever your device is turned on . . . Sprint offers unique features to its users, including a number of location-enabled services that you activate and use. To provide these services, the Sprint network must use the location information of your device to deliver your services . . . You should carefully review the terms and conditions and privacy policies of third party application and service providers to understand their use [*73] of your location information. Only share your location information with those you trust. It is your responsibility to inform anyone that uses your wireless device and all of the users of other wireless devices on your account of location capabilities and the location based services that are in use for those devices.

Id.

In addition, there has been an explosion of articles in the press on GPS and cell site tracking by law enforcement. Chief Judge Kozinski's recent dissent in Pineda-Moreno highlights the controversy and concerns about "the tidal wave of technological assaults on our privacy." *Pineda-Moreno, 617 F.3d at 1125* (Kozinski, C.J., dissenting from the denial of reh'g en banc). He cites articles in the mainstream media and blogs sounding the alarm about the volume and intrusiveness of law enforcement access to cell phone users' location data. See id. Various foundations and advocacy groups have also weighed in, expressing reservation about unbridled and unsupervised law enforcement use of evolving technologies, especially for cell phone location tracking. See, e.g., ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/cell-tracking (last visited May 6, 2011) (describing advocacy [*74] efforts with regard to warrantless cell phone location tracking); CENTER FOR DEMOCRACY AND TECHNOLOGY, http://www.cdt.org/issue/location-privacy (last visited May 6, 2011) (gathering resources on location privacy); DIGITAL DUE PROCESS COALITION, http://digitalddueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited May 6, 2011) (stating that the overarching goal of the coalition is "to simplify, clarify, and unify the ECPA standards, providing stronger privacy protections for communications and associated data in response to changes in technology and new services and usage patterns, while preserving the legal tools necessary for government agencies to enforce the laws, respond to emergency circumstances and protect the public").

In the last year there has been considerable congressional investigation regarding the privacy of location data and other electronic information and, in particular, in response to media coverage of law enforcement use of electronic surveillance and calls for examination and reform of the Electronic Communications Privacy Act ("ECPA"). Written when communication was mostly done over land-line phones, it is generally agreed that ECPA [*75] has not kept pace with rapidly evolving technology. Steve Titch, TITCH: Block Big Brother's Internet Snoops, THE WASHINGTON TIMES (May 26, 2011, 7:20 PM), http://www.washingtontimes.com/news/2011/may/26/block-big-brothers-internet-snoops/ (last visited July 21, 2011). Because ECPA was not enacted with this specific technology in mind, it has been criticized as providing only confusing guidelines, with the situation exacerbated by federal courts' conflicting decisions on the constitutionality of these and other related requests. Gina Stevens, Alison M. Smith, & Jordan Segall, Legal Standard for Disclosure of Cell-Site Information (CSI) and Geolocation Information, CONGRESSIONAL RESEARCH SERVICE (Jun. 29, 2010).

Congress has held six hearings since 2010 on the technology and law of electronic surveillance, including several with a particular focus on ECPA. [14] These hearings demonstrate congressional concern about the privacy implications of increased access to location information and other rapidly evolving technologies, while recognizing the legitimate needs of law enforcement. See, e.g., Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil [*76] Rights, and Civil Liberties, of the H. Comm. on the Judiciary, 11th Cong. (May 5, 2010). In his opening remarks at one of these congressional hearings on ECPA reform, Representative Nadler, Chair of the Subcommittee on the Constitution, Civil Rights, and Civil Liberties, queried:

> How do current advances in location technology test traditional standards of the ECPA of 1986? More generally, in what ways have these and other technologies potentially subverted one of the original and central goals of ECPA, which was to preserve a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement?

Id. at 2 (internal quotations omitted).

> 14 These six Congressional hearings include: Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. (May 5, 2010) (discussing need for reform of the ECPA in light of new communications technologies); ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. (Jun. [*77] 24, 2010) (examining the need to update the ECPA with a particular focus on cell site information and other location based technologies); The Electronic Communications Privacy Act -- Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary, 111th Cong. (Sept. 22, 2010) (examining the need to update the ECPA in light of advances in communications technologies); ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. (Sept. 23, 2010) (discussing the need to update the ECPA with a particular focus on cloud computing); The

Electronic Communications Privacy Act -- Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary, 111th Cong. (Apr. 6, 2011) (discussing how the need to update the ECPA affects the government's ability to fight crime and protect national security); Protecting Mobile Privacy -- Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the Hearing Before the S. Comm. on the Judiciary, 111th Cong. (May 10, 2011) (discussing the privacy [*78] implications of smartphones and other mobile applications).

In apparent response to this very issue, three bills that would amend ECPA have been introduced in Congress during a one-month interval between May and June of 2011. [15] On May 17, 2011, Senator Patrick Leahy (D-VT), Judiciary Committee Chairman and original author of EPCA, introduced the Electronic Communications Privacy Act Amendments Act of 2011 ("Leahy Bill"), a comprehensive bill that would require, inter alia, that the government obtain a search warrant in order to access real-time geolocation information, and a search warrant or order to obtain historical geolocation information, from an electronic communications, remote computing, or geolocation information service provider. S. 1011, 112th Cong. (2011); Summary of Electronic Communications Privacy Act Amendments Act of 2011 and Press Release, SENATOR LEAHY'S WEBSITE (May 17, 2011), http://leahy.senate.gov/press/press_releases/release/?id=b6d1f687-f2f7-48a4-80bc-29e3c5f758f2#Summary.

15 While there has been considerable congressional activity around ECPA reform recent months, as demonstrated by the hearings and bills discussed here, congressional concern over ECPA and location [*79] privacy is not new. For example, Representative Charles Canady introduced a bill during the 106th Congress in 2000 that sought to amend ECPA, *18 U.S.C. ß 2703*, to require that "a provider of mobile electronic communication service shall provide to a government entity information generated by and disclosing the current physical location of a subscriber's equipment only if the governmental entity obtains a court order issued upon a finding that there is probable cause..." H.R. 5018, 106th Cong. (2000) (as reported by H. Comm. on the Judiciary, Oct. 4, 2000).

On June 15, 2011, Senators Al Franken (D-MN) and Richard Blumenthal (D-CT) introduced the Location Privacy Act of 2011 ("Franken Bill"), seeking to close perceived loopholes in federal law by requiring any company that may obtain a customer's location information from a mobile device to get that customer's express consent before collecting his or her location data or sharing his or her location data with third parties. S. 1223, 112th Cong. (2011); The Location Privacy Protection Act of 2011 Bill Summary, SENATOR FRANKEN'S WEBSITE (Jun. 15, 2011), http://franken.senate.gov/files/docs/110614_The_Location_Privacy_Protection_Act_of_2011_One_pager.pdf. [*80] While this bill notably applies only to non-governmental entities, it underscores the shortcomings of ECPA as well as congressional concern about the privacy implications of location data.

Also on June 15, 2011, Senator Ron Wyden (D-OR) and Representative Jason Chaffetz (R-UT) introduced the Geolocational Privacy and Surveillance or "GPS" Act ("Wyden Bill"), a bill seeking to address the growing concern that there are no clear rules governing how law enforcement, commercial entities and private citizens can access, use and sell location data. H.R. 2168, 112th Cong. (2011); Wyden, Chaffetz Introduce Geolocation Privacy and Surveillance ("GPS") Act, SENATOR WYDEN'S WEBSITE (Jun. 15, 2011), http://wyden.senate.gov/issues/issue/?id=b29a3450-f722-4571-96f0-83c8ededc332#sections. The Wyden Bill specifically requires a warrant for the

acquisition of geolocation information, subject to a list of exceptions, namely emergency situations. Id. The bill covers both real-time tracking and access to records of individuals' past movements in the same way and establishes guidelines for both law enforcement agencies and private entities that have access to geolocation information. Id.

These bills do not [*81] establish a different proof for location data depending on law enforcement purpose in acquisition. The bills clearly do not recognize any Payton exception to the warrant requirement where location data is sought to effect an arrest.

In opposition to the bill, the DOJ has argued that using electronic data to track a person's movements is akin to human surveillance (i.e., following a person walking down the street), which is legal, and should be treated the same. Id. Senator Wyden wrote that "tracking an individual's movements on [a] twenty-four hour basis for an extended period of time [as made possible by electronic tracking] is qualitatively different than visually observing that person during a single trip, and can reveal significantly more information about their activities and pattern of life." Id. In addition, "tracking an individual with a GPS device or by tracking their cell phone is much cheaper and easier than tracking them with a surveillance team, so the resource barriers that act as a check against abuse of visual surveillance techniques do not always apply to geolocation tracking and other electronic surveillance methods." Id. [16]

16 Demonstrating similar concern, a number [*82] of state legislatures have prohibited use of electronic tracking devices except pursuant to a search warrant. See *Maynard, 615 F.3d at 564* ("...states have enacted legislation imposing civil and criminal penalties for the use of electronic tracking devices and expressly requiring exclusion of evidence produced by such a device unless obtained by the police acting pursuant to a warrant."). The Maynard court noted that "the Legislature of California, in making it unlawful for anyone but a law enforcement agency to use an electronic tracking device to determine the location or movement of a person, specifically declared that electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy, and implicitly but necessarily thereby required a warrant for police use of a GPS." Id. (citing *California Penal Code section 637.7*, Stats.1998 c. 449 (S.B.1667) ß 2 (internal quotations omitted). The Maynard court cited similar electronic tracking statutes from Utah, Minnesota, Florida, South Carolina, Oklahoma, Hawaii, and Pennsylvania which provide for exclusion of evidence obtained by an electronic tracking device where law enforcement [*83] fails to obtain ex ante judicial approval in the form of a warrant. Id. (citing *Utah Code Ann. ßß 77-23a-4*, *77-23a-7*, *77-23a-15.5*; *Minn. Stat. ßß 626A.37*, *626A.35*; *Fla. Stat. ßß 934.06*, *934.42*; *S.C. Code Ann. ß 17-30-140*; *Okla. Stat. tit. 13, ßß 176.6*; *Haw. Rev. Stat. ßß 803-42*, *803-44.7*; *18 Pa. Cons. Stat. ß 5761*).

This legislation, both proposed and enacted, demonstrates recognition of the dangerously intrusive nature of cell phones as tracking devices and confines them to use in the most basic, core function of government: to ferret out crime and provide a safe society for its citizens. See id. (opining that "[a]lthough perhaps not conclusive evidence of nationwide "societal understandings," *Jacobsen, 466 U.S. at 123 n.22, 104 S.Ct. 1652*, this legislation is indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable.); see also Michael Isikoff, The Snitch in Your Pocket, NEWSWEEK (Mar. 1, 2010), available at http:// www.newsweek.com/id/233916 (discussing controversy over U.S. government surveillance of cellular telephone conversations and records and considering concerns about civil liberties and the

individual right to privacy); [*84] Christopher Soghoian, 8 Million Reasons for Real Surveillance Oversight, SLIGHT PARANOIA (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (last visited Jul. 21, 2011) (reporting that Sprint Nextel provided law enforcement agencies with its customers' GPS location information over 8 million times between September 2008 and October 2009, and that this massive disclosure of sensitive customer information was made possible due to the roll-out by Sprint of a new, special web portal for law enforcement officers); Justin Scheck, Stalkers Exploit Cellphone GPS, WALL ST. J. (Aug. 5, 2010), at A1, A14 (reporting that identifying AT&T and Verizon as providing "law-enforcement[ ] easy access to such data"); Spencer Ackerman, Bill Would Keep Big Brother's Mitts Off Your GPS Data, WIRED.COM, http://www.wired.com/dangerroom/2011/05/bill-would-keep-big-brothers-mitts-off-your-GPS-Data 6/23/2011 (last visited Jul. 21, 2011) (reporting on Wyden/Chaffetz bill and quoting Rep. Chaffetz as stating that "We [do not] want law enforcement to be able to follow everyone all the time.").

Against this backdrop of intense congressional inquiry and public concern, [*85] it is especially inappropriate to sanction an expansion of law enforcement acquisition of location data on a wishful but unsupported view of Payton.

So, having found neither precedential nor doctrinal support for the government's reliance on the arrest warrant alone as authority for its location data request, the Court considers whether this is a permissible search under the *Fourth Amendment* and *Rule 41*.

d. There is no Clear Authority Under the *Fourth Amendment* for a Search Warrant for Location Data to Aid in Apprehension of a Subject of an Arrest Warrant Absent Flight

At the outset, it should be clear what the government is seeking (and not seeking) under the *Fourth Amendment* and *Rule 41*. The government is not seeking a warrant to search for the defendant in a particular place. As discussed infra, that, of course, would be permissible on probable cause. Nor is the government seeking a warrant to seize the defendant; the arrest warrant already authorizes the government to do that. The government is seeking a warrant for location data from the defendant's cell phone for as long as 30 days on a showing of reasonable belief that the cell phone belongs to him and is in his possession. (ECF [*86] No. 15, 20).

Having found that the government's request constitutes an invasion into a constitutionally-protected area of privacy and that under current law the arrest warrant alone does not authorize acquisition of location data, the Court now examines whether the government has satisfied the constitutional requirements to conduct such a search for location data under the *Fourth Amendment*.

In all areas in which a person has a reasonable expectation of privacy, he is protected from "unreasonable searches and seizures." *U.S. CONST. amend. IV*. The *Fourth Amendment* does not require that a warrant be obtained for all searches, however. *United States v. Rabinowitz, 339 U.S. 56, 66, 70 S. Ct. 430, 94 L. Ed. 653 (1950)*. What constitutes a "reasonable" search and seizure derives content and meaning through reference to the warrant clause and, unless an exception applies, the government must "obtain advance judicial approval of searches and seizures through a warrant procedure." *United States v. U.S. District Court, 407 U.S. 297, 315, 92 S. Ct. 2125, 32 L. Ed. 2d 752 (1972)*; *Coolidge v. New Hampshire, 403 U.S. 443, 473-84, 91 S. Ct. 2022, 29 L. Ed. 2d 564 (1971)*; *Terry v. Ohio, 392 U.S. 1, 20, 88 S. Ct. 1868, 20 L. Ed. 2d 889 (1968)*.

The government does not contend explicitly that the search for and seizure of location information [*87] is "reasonable" under the first clause of the amendment, or that it falls within any exception to the warrant requirement. See *Katz v. United States, 389 U.S. 347, 357, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)*; LAURIE LEVENSON, FED. CRIM. RULES HANDBOOK FCRP 41 n.21 (2009 ed.)(listing recognized exceptions to the *Fourth Amendment* warrant requirement). Indeed, the government has presented no grounds for such an exception, and it clearly does not fall within a recognized exception. This is not to say that the Supreme Court might not determine that this search should be analyzed under the "reasonableness standards of Clause 1," and that location data may be obtained on a showing less than or different than probable cause that the search will reveal evidence of a crime and that "advance judicial approval" is not required. However, the government has not argued, and the Court cannot discern, the precedential basis for such a ruling aside from an unsupported expansion of Payton, which the Court has already rejected. As the Supreme Court stated in *Skinner v. Railway Labor Executives' Association, 489 U.S. 602, 619, 109 S. Ct. 1402, 103 L. Ed. 2d 639 (1989)*, "the permissibility of a particular practice 'is judged by balancing its intrusion on the individual's [*88] *Fourth Amendment* interests against its promotion of legitimate government interests.' In most criminal cases, we strike this balance in favor of the procedures described by the Warrant Clause of the *Fourth Amendment*." (internal citations omitted).

The Court as a rule examines "criminal" searches under the Warrant Clause and "civil" searches under the Reasonableness Clause. Fabio Arcila, Jr., In the Trenches: Searches and the Misunderstood Common Law History of Suspicion and Probable Cause, *10 U. PA. J. CONST. L. 1, 10 (2007)*; CONG. RESEARCH SERV., THE CONSTITUTION OF THE UNITED STATES OF AMERICA: ANALYSIS AND INTERPRETATION, S. Doc. No. 108-17 at 1286 (2d Sess. 2004) ("ANALYSIS AND INTERPRETATION"). While the "special needs" doctrine applies in some law enforcement-related circumstances, its applicability requires the existence of circumstances "beyond the normal needs for law enforcement." *Chandler v. Miller, 520 U.S. 305, 313-14, 117 S. Ct. 1295, 137 L. Ed. 2d 513 (1997)*. Compare *Michigan Dep't of State Police v. Sitz, 496 U.S. 444, 451, 110 S. Ct. 2481, 110 L. Ed. 2d 412 (1990)* (holding that sobriety checkpoints constitute permissible warrantless searches), with *City of Indianapolis v. Edmond, 531 U.S. 32, 35, 40-41, 121 S. Ct. 447, 148 L. Ed. 2d 333 (2000)* (holding that roadside checkpoints [*89] aimed at enforcing drug laws are not permissible warrantless searches). The government alleges no facts that take it outside of the context of normal law enforcement investigation and within any recognized exception, including the special needs doctrine. The government's argument under Payton, if accepted, would create another "special exception," relieving law enforcement of the obligation to seek prospective judicial approval before the search under the second clause of the *Fourth Amendment* subject to challenge as "unreasonable" under the first clause if law enforcement did not have probable cause to believe that the defendant was the subject of an arrest warrant, that he had a cell phone and was in possession of that cell phone. The circumstances here do not come within any recognized exception, nor do they meet the articulated test for such an exception. See *Griffin v. Wisconsin, 483 U.S. 868, 873, 107 S. Ct. 3164, 97 L. Ed. 2d 709 (1987)* (quoting *New Jersey v. T.L.O., 469 U.S. 325, 351, 105 S. Ct. 733, 83 L. Ed. 2d 720 (1985)* (Blackmun, J., concurring in judgment)) ("[W]e have permitted exceptions when 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'"). [17] Or as Justice [*90] Blackmun articulated the "special needs" trigger: "[O]nly when the practical realities of a particular situation suggest that a government official cannot obtain a warrant based on probable cause without sacrificing the ultimate goals to which the search would contribute, does the Court turn to a 'balancing' test to formulate a standard of reasonableness for this context." *O'Connor v. Ortega, 480 U.S. 709, 741, 107 S. Ct. 1492, 94 L.*

Ed. 2d 714 (1987) (Blackmun, J., dissenting). The government did not argue that the warrant and probable cause requirement was "impracticable." Rather, the government argued under Payton that the warrant and probable cause requirement was constitutionally unnecessary. There was no demonstrated impracticability -- inconvenience perhaps -- but no more.

17 The Griffin holding -- that search of a probationer's home, pursuant to Wisconsin regulation requiring only reasonable grounds and no prior judicial approval is clearly distinguishable here, as it involved a person convicted of a crime and still under supervision. Also, the Supreme Court found impracticability: "A warrant request would interfere to an appreciable degree with the probation system, setting up a magistrate rather than the probation [*91] officer as the judge of how close a supervision the probationer requires. Moreover, the delay inherent in obtaining a warrant would make it more difficult for probation officials to respond quickly to evidence of misconduct . . . and would reduce the deterrent effect that the possibility of expeditious searches would otherwise create." *Id. at 876* (citations omitted). Lastly, the Court noted that "[a]lthough a probation officer is not an impartial magistrate, neither is he the police officer who normally conducts searches against the ordinary citizen . . . and is supposed to have in mind the welfare of the probationer. . . ."

It may well be that the Supreme Court will extend Payton to find that a search warrant is unnecessary under these circumstances and that the privacy rights of the subject of the arrest warrant may be adequately assured after-the-fact by application of the exclusionary rule or civil remedies, where available. [18] However, the Court does not see any clear doctrinal path to the relief the government seeks. Therefore, the *Fourth Amendment* requires the government to meet the probable cause standard of the second clause of the *Fourth Amendment* to obtain a search warrant [*92] for location data. In any event, the government sought a warrant herein, though it did so only because the telecommunications carrier required a warrant to execute the search for the location data.

18 For instance, the arrestee could invoke the exclusionary rule to suppress evidence obtained by the government as a result of a defective arrest warrant or impermissible warrantless arrest. See *Mapp v. Ohio, 367 U.S. 643, 81 S. Ct. 1684, 6 L. Ed. 2d 1081, 86 Ohio Law Abs. 513 (1961)* (holding that evidence obtained in violation of the *Fourth Amendment* may not be used in criminal prosecutions in state or federal courts). In addition, the arrestee under certain circumstances could bring a civil action for damages based on state common law (i.e., false arrest or false imprisonment) or constitutional tort. See *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 91 S. Ct. 1999, 29 L. Ed. 2d 619 (1971)* (holding that a violation of the *Fourth Amendment* by a federal agent acting under color of law gives rise to a cause of action for damages); *Monroe v. Pape, 365 U.S. 167, 172, 81 S. Ct. 473, 5 L. Ed. 2d 492 (1961)* (explaining that *42 U.S.C.S. ß 1983* "gives a remedy to parties deprived of constitutional rights, privileges and immunities by an official's abuse of his position."). Notably, though, [*93] cases in which the Supreme Court has set aside a conviction due to a defective arrest warrant are exceedingly rare. See, e.g., *Giordenello v. United States, 357 U.S. 480, 78 S. Ct. 1245, 2 L. Ed. 2d 1503 (1958)* (setting aside a conviction verdict due to an invalid arrest warrant); *West v. Cabell, 153 U.S. 78, 86, 14 S. Ct. 752, 38 L. Ed. 643 (1894)* (explaining that a police officer has no authority to arrest if the warrant is defective).

Where a warrant is required for a search, as it is here, the Court may issue one only upon the government's showing of "probable cause." The parties vehemently disagree as to the requisite nature of the "probable cause" showing under the *Fourth Amendment*. The government largely acknowledges that it must meet the probable cause (or reasonable belief) standard but asserts that, there is probable cause here that the evidence sought will aid in a particular apprehension and that is sufficient. (ECF No. 6, 3; ECF No. 10, 2).

Interestingly, testimony in the May 5, 2010 congressional hearing framed the exact issue faced here. In responding to a proposal that the law clearly establishes that "location information regarding a mobile communications device [can be obtained] only with a warrant issued based on a showing of probable [*94] cause," Professor Orin Kerr asked:

> . . . **[P]robable cause of what?** Is that probable cause to believe the person tracked is guilty of a crime? Or is it probable cause to believe the evidence of location information obtained would *itself* be evidence of a crime?
>
> The difference is important. **In the case of a search warrant, "probable cause" generally refers to probable cause to believe that the information to be obtained is itself evidence of a crime.** But cell phone location information will itself be evidence of crime only in specific kinds of cases. For example, **such information normally will not be evidence of a crime if investigators want to obtain the present location of someone who committed a past crime.**
>
> To see this, imagine the police have probable cause to arrest a criminal for a crime committed last week. The police want to locate the suspect in order to arrest him. In that case, the police will not have probable cause to believe that the location of the criminal's cell phone is itself evidence of a crime. The suspect's location a week after the crime occurred does not give the police any information indicating that the suspect did or did not commit the crime. But if the police [*95] have probable cause to arrest someone, and they know his cell-phone number, I would think the law should allow the government some way of locating the suspect pursuant to an appropriate court order. A requirement that location information be obtainable only based on probable cause to believe that the location information is itself evidence of a crime would not seem to allow that.

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. 39-40 (2010) (statement of Orin Kerr, Professor, George Washington Univ. Law School) ("Kerr Testimony")(emphasis in original; bolding added). While Professor Kerr appears to believe that law enforcement should be able to use location data in aid of the apprehension of a defendant, he acknowledged that "probable cause" under current *Fourth Amendment* jurisprudence "generally refers to probable cause to believe that the information to be obtained is itself evidence of a crime." Id. As discussed below, this Court agrees.

The government's contrary definition of probable cause relies almost exclusively on its reading of *Warden v. Hayden, 387 U.S. 294, 87 S. Ct. 1642, 18 L. Ed. 2d 782 (1976)*: [*96] no nexus between the subject of a search warrant and criminal behavior is necessary; a search warrant can be

issued to aid in the apprehension of a criminal defendant. (ECF No. 6, 3; ECF No. 10, 2). The Federal Public Defender interprets Warden v. Hayden entirely differently, arguing that the government, "when applying for a search warrant, must establish a reasonable probability that the information it seeks to obtain constitutes proof of a crime." (ECF No. 8, 3). The Court agrees with the Federal Public Defender's reading of the holding in Warden v. Hayden. However, other authorities convince the Court that a warrant can be issued to search for the subject of an arrest warrant, if the government has probable cause to believe that he is in a particular place. But if the government does not have probable cause to believe that the subject of an arrest is in a particular place, a warrant can only issue under the second clause of the *Fourth Amendment* if there is probable cause he has fled prosecution, that is, that his location is evidence of a crime. See *18 U.S.C. ß 1073*.

As both parties correctly recognize, Hayden is a landmark case that rejects, for purposes of the warrant requirement, [*97] any distinction between "mere evidence" and instrumentalities, fruits, or contraband of crime. (ECF No. 8; ECF No. 10, 2). Specifically, Hayden held that the *Fourth Amendment* equally governs searches for "mere evidence" and searches for instrumentalities, fruits, or contraband of crime. *Hayden, 387 U.S. at 306-07*. However, the government focuses on particular language in Hayden: "probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction." *Id. at 307*. The Federal Public Defender trumpets other language in the opinion: "there must be a nexus ... between the items to be seized and criminal behavior." Id. However, a close examination of the facts of Hayden demonstrates the correctness of the Federal Public Defender's interpretation. The language upon which the government relies, is properly viewed as dicta-intriguing dicta-but dicta. In Hayden, the issue was the admissibility of articles of clothing to connect the defendant to the criminal activity and thus convict him. Police were notified that an armed robber wearing a light cap and dark jacket had entered a house. Police, on entering, found the defendant [*98] and in the search of the house, found a light cap and dark jacket in a washing machine in the house. While the opinion does indeed state that "probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction, *id. at 307*, the facts of the case involve use of these items to convict the man in the house where the clothes were found, not to apprehend him.

Moreover, the government admitted at the hearing it was unable to provide any explicit substantive support for its reading of Hayden in factually apposite cases, treatises or law reviews. [19] Rather, the government cites to language in *Andresen v. Maryland, 427 U.S. 463, 96 S. Ct. 2737, 49 L. Ed. 2d 627 (1976)*, and *Dalia v. United States, 441 U.S. 238, 99 S. Ct. 1682, 60 L. Ed. 2d 177 (1979)*, in an attempt to establish that Hayden did not advance an absolute nexus requirement, alleging that these two cases "did not even bother to repeat Hayden's nexus language." (ECF No. 10, 2 n.1). However, it is not use of the precise word "nexus" that embodies the requirement -- it is the principle that the object of the search must relate to the crime. Indeed, in both of these cases there was a factual nexus between criminal activity and the searched-for [*99] items. Andresen applied the nexus standard, interpreting a warrant to authorize seizure of evidence only to the extent that it established probable cause that the documents were related to the suspect crime. *Andresen, 427 U.S. at 481-83*. Similarly, Dalia approved issuance of a warrant that allowed the government to plant a "bug" in a suspect's office where the magistrate judge found probable cause to believe that the suspect was committing specific federal crimes, that he was using his office in connection with those crimes, and that bugging his office would lead to interception of oral communications concerning those crimes. *Dalia, 441 U.S. at 241-42, 256*. Legal pronouncements do not live isolated

from the facts; they can only be understood in the context of the facts presented. The Court could find no case where a search warrant was issued to obtain information to aid in the apprehension of a criminal where the sought-for information would not be evidence of a crime.

> 19 Indeed, the response to Hayden of the Advisory Committee on Criminal Rules is instructive on this point. The Committee did not seek to amend *Rule 41* to clarify that a search warrant may be used to obtain evidence that [*100] will aid in the apprehension of a defendant. Rather, the Committee queried: "One question is whether it is desirable to amend *Rule 41(b)* to provide that search warrants may issue for evidence of the commission of a crime and if it is, whether this is the way to do it. [Professor Remington] said that the Department of Justice had said that it might be desirable to amend the rule to reflect the Hayden case." ADVISORY COMM. ON CRIM. RULES, MINUTES OF THE SEPTEMBER 1967 MEETING OF THE ADVISORY COMM. ON CRIM. RULES 2 (Sept. 11-12, 1967), available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Minutes/CR09-1967-min.pdf. And, indeed, *Rule 41* was amended consistent with the Committee and the FPD's view of the Hayden holding. See *FED. R. CRIM. P. 41*, Advisory Committee's Note, 1972 Amendments ("*Subdivision (b)* is also changed to . . . take account of a recent Supreme Court decision (*Warden v. Hayden, 387 U.S. 294, 87 S. Ct. 1642, 18 L. Ed. 2d 782 (1967))* and recent Congressional action (*18 U.S.C. ß 3103a*) which authorize the issuance of a search warrant to search for items of solely evidentiary value.").

In short, the government has not overcome this longstanding principle of law. The *Fourth Amendment's* standard [*101] of probable cause for searches and seizures has a firmly embedded nexus component. See *Dumbra v. United States, 268 U.S. 435, 441, 45 S. Ct. 546, 69 L. Ed. 1032 (1925)* ("In determining what is probable cause . . . [w]e are concerned only with the question whether the affiant had reasonable grounds at the time of his affidavit . . . for the belief that the law was being violated on the premises to be searched."). While warrants are no longer limited to only contraband and the fruits and instrumentalities of crime, they must still be specifically tailored to permit search or seizure only of things and places that have a connection to the alleged criminal activity. See, e.g., *Zurcher v. The Stanford Daily, 436 U.S. 547, 557 n.6, 98 S. Ct. 1970, 56 L. Ed. 2d 525 (1978)* (quoting Comment, 28 U. Chi. L. Rev. 664, 687 (1961) (footnotes omitted in original) (noting that valid warrants must be supported by "'substantial evidence[] that the items sought are in fact seizable by virtue of being connected with criminal activity, and that the items will be found in the place to be searched.'"). See also *Doe v. Broderick, 225 F.3d 440 (4th Cir. 2000)* (citing *Warden, 387 U.S. at 307*) (invalidating a search warrant where an officer's declaration failed to establish [*102] a "nexus between the items to be seized and the criminal activity being investigated"); see also WILLIAM E. RINGEL, SEARCHES AND SEIZURES, ARRESTS AND CONFESSIONS, ß 2:8 (2d ed. 2010) (noting that nexus requirement is the only requirement for seizure of an article of mere evidence over and above constitutional requirements); John M. Burkoff, Search Warrant Law Deskbook, ßß 18:1 (Dec. 2009) ("[e]videntiary items, including papers and documents, that are specified in a search warrant or inadvertently discovered in plain view during the execution of a search warrant lawfully may be seized, provided that it is immediately apparent to the seizing officers that the items are those described in the warrant or that they otherwise possess a nexus with criminal activity").

While the government could point to no specific case approving the use of a warrant to search for the subject of an arrest warrant, there can be little question that a warrant can be obtained to

search for and seize such a person. Moreover, Payton and Steagald have delineated some of the circumstances when a warrant must be obtained to search for and seize such a person. In a 1974 law review article, Professor Daniel Rotenberg [*103] brilliantly and incisively identified the incongruence between the development of the law on search warrants and arrest warrants:

> Generally, arrest warrants require designation or description of the person to be arrested with no reference to the places that may be searched in effecting the arrest. Search warrants, on the other hand, require a specific description of the place to be searched as well as the property sought with no reference to persons sought. This means that if the object of the search is a person, neither arrest nor search warrant rules fit. There is thus no established procedure that complies with the constitutional mandate that "no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons . . . to be seized.

Daniel L. Rotenberg & Lois B. Tanzer, Searching for the Person to Be Seized, 35 OHIO ST. L.J. 56, 57-58 (1974).

Shortly thereafter, the Criminal Rules were amended to add *clause (4)* to then *Rule 41(b)* allowing a warrant to search for and seize a person for whose arrest there is probable cause. As noted in WRIGHT, KING, & KLEIN, "At the time the 1979 amendment was being formulated, there was uncertainty [*104] whether a warrant was needed to enter private premises to make an arrest." 3A FEDERAL PRAC. & PROC. CRIM. ß 664.1 (3d ed. 2009). After Steagald, the treatise continued "it may be that there will be few circumstances in which this holding will be applicable but it was wise that the amendment did provide a procedure for those circumstances." Id. Statutory law at the time also suggested plenary authority of law enforcement to search private dwellings, solely on the basis of an arrest warrant. See *18 U.S.C. ß 2236 (1970)*.

> [W]hoever, being an officer, agent or employee of the United States or any department or agency thereof, engaged in the enforcement of any law of the United States searches any private dwelling used and occupied as such dwelling without a warrant directing such search . . . shall be fined . . . or imprisoned . . . . This section shall not apply to any person a) serving a warrant of arrest; or b) arresting or attempting to arrest a person . . .

Thus, the use of a search warrant to apprehend a person for whose arrest there was probable cause was codified. See Orders of the Supreme Court of the United States Adopting and Amending Rules, Order of April 30, 1979 (approving amendments [*105] to *Rule 41* and transmitting them to Congress in accordance with *18 U.S.C. ßß 3771*, *3772*).

To be clear, no one is questioning the use of a search warrant to apprehend a criminal defendant where the government can present probable cause that the defendant is in a particular place. Rather, the government's request here is for broad information concerning defendant's ongoing location. Unlike in investigations of ongoing crimes, the government here alleges no relationship whatsoever between defendant's ongoing movements and his crime. Cf. *United States v. Garcia-Villalba, 585 F.3d 1223, 1234 (9th Cir. 2009)* (recognizing that a defendant's physical movements from place to

place satisfied sufficient nexus where defendant was suspected of ongoing drug trafficking); *United States v. Rojas, 671 F.2d 159, 165 n.8 (5th Cir. 1982)* ("[W]arrants are issued for surveillance or tracking devices on probable cause that the 'search' (the surveillance or tracking) will uncover evidence of a crime"). Because the government has not established the requisite nexus between the information sought and an alleged crime, no search warrant may issue for this location data. Additionally, the government has not provided [*106] any authority for its probable cause definition in this circumstance -- probable cause that the subject of an arrest warrant is using a specified wireless telephone. While that would seem to be a reasonable showing, aimed at a laudable societal goal of bringing a charged individual to justice, it is an exercise of police power neither clearly envisioned in the *Fourth Amendment* nor approved by the courts, in an area of quickly shifting, complex technology. Moreover, it is akin to general investigatory activity, for which search warrants are not issued.

As Professor Kerr queried in his congressional testimony:

> But if the police have probable cause to arrest someone, and they know his cell-phone number, **I would think the law should allow the government some way of locating the suspect pursuant to an appropriate court order.** A requirement that location information be obtainable only based on probable cause to believe that the location information is itself evidence of a crime **would not seem to allow that.**

Kerr Testimony at 39-40 (emphasis added). While Professor Kerr identified this issue, he did not provide any solution in constitutional jurisprudence. Nor has any lawmaker in any of the pending [*107] legislative proposals discussed earlier suggested a constitutional or statutory clarification or fix to allow this use of location data; the "Wyden Bill" and the "Leahy Bill" establish unequivocally that prospective, real time location data can only be acquired through a warrant. [20]

> 20 Under the Leahy Bill, the government must get a search warrant to access contemporaneous (real-time) geolocation information from an electronic communications, remote computing, or geolocation information service provider, and either a search warrant or court order, issued on a showing of specific and articulable facts that there are reasonable grounds to believe the information is relevant and material to an ongoing criminal investigation, to obtain historical geolocation information from the same providers. S. 1011, 112th Cong. (2011). Therefore, in this case, under the Leahy Bill, the government would have to show probable cause and get a search warrant to access the "real time" data it requests. The Wyden Bill similarly requires the government to get a search warrant before it can obtain location data from a "wireless communication device," such as a cell phone. S. 1212, 112th Cong. (2011). It would [*108] require the government to get a search warrant when it wants to acquire an individual's geolocation information from a private company or monitor an individual's movements directly, using covertly installed tracking devices or similar means. Id. Notably, this bill also prohibits unlawfully intercepted geolocation information from being used as evidence. Id..

In any event, case law does not provide a way forward -- a firm constitutional basis for issuance of a warrant here. Thus, a warrant is unavailable where there is no evidence of flight.

Our analysis could, of course, stop here. The government's other authorities -- *Rule 41*, the Stored Communications Act, the inherent authority of the Court, and the All Writs Act -- are subservient to the *Fourth Amendment*. However, the Court will discuss the government's other arguments for its entitlement to a warrant and provide guidance as to the circumstances under which a warrant may issue for the subject of an arrest warrant.

2. *Rule 41*

Recognizing that *Rule 41* governs all search warrants, the government makes several, alternative arguments as to how its request squares with the terms of the rule, and more generally contends that its request is "consistent [*109] with *Rule 41*." (ECF No. 6, 5; ECF No. 10, 4-5). The government argues that the four categories of warrants provided for in *Rule 41(c)* are not intended to be exclusive, and that law enforcement may conduct searches or seizures that do not fall within the itemized categories without violating the *Fourth Amendment*. (ECF No. 6, 5). The government therefore urges the Court to read the *Rule 41(c)* categories "broadly" and "flexibly." (Id. at 5-6; ECF No. 10, 4-5). In its last submission to the Court, the government asserts without supporting authority that *Rule 41(c)(4)* "authorizes a search for a person to be arrested" and "[a]lthough the location information sought in this case is not itself a person to be arrested, it properly falls within the scope of a search warrant for a person to be arrested ..." (ECF No. 10, 5). Alternatively, the government contends, because *Rule 41* does not "specifically address" a warrant for the requested information, the Court has inherent authority to issue the search warrant and the All Writs Act vests the Court with adequate authority to take steps to "effectuate an arrest warrant." (ECF No. 6, 4-5; ECF No. 10, 6-8). [21] Finally, the government argues that "[no [*110] procedural rule prevents this Court from issuing as warrant for evidence that will aid in an apprehension." (ECF No. 6, 3). That position is wrong-headed. *Rule 41* sets out the procedures required in implementation of the *Fourth Amendment*, and the government has failed to bring its request within the *Fourth Amendment* and within the rule's provisions. The Court finds all of the government's arguments under *Rule 41* unavailing.

> 21 The government's All Writs Act argument is addressed in greater detail later in this opinion, but it bears noting here that *Rule 41* does indeed address the situation at hand -- the government may obtain the precise location information it seeks pursuant to a *Rule 41(c)(1)* warrant for information constituting evidence of a crime, as long as it meets the required probable cause standard. Here, it does not.

The search warrant standard codified in the Federal Rules of Criminal Procedure is rooted in the *Fourth Amendment*, and is intended to articulate and implement *Fourth Amendment* principles, not to expand or change the *Fourth Amendment* parameters. The Rules were adopted in 1944 to collect and streamline existing practices and procedures that were fundamentally sound, [*111] but haphazard, located in many cases and not set out in one written document, and confusing in form. See James J. Robinson, The Proposed Federal Rules of Criminal Procedure, 27 J. AM. J. SOC. 38, 39 (1943); Lester B. Orfield, The Preliminary Draft of the Federal Rules of Criminal Procedure, 22 TEX. L. REV. 37, 42 (1943). The Federal Rules of Criminal Procedure established uniform procedures to which all federal courts were thereafter required to adhere. *FED. R. CRIM. P. 1(a)(1)*.

Like the rules of criminal procedure generally, *Rule 41* was incepted to codify and clarify search and seizure practice and procedure as it existed in 1944 and before. Thus, the rule adopted the existing statutory warrant procedure which, in turn, had been based on existing law. See ADVISORY

COMM. ON RULES OF CRIMINAL PROCEDURE, MINUTES OF MEETINGS OF ADVISORY COMMITTEE ON RULES ON CRIMINAL PROCEDURE 883 (Feb. 23, 1943) available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Minutes/ CR02-1943-min-Part3.pdf.pdf; ADVISORY COMM. ON RULES OF CRIMINAL PROCEDURE, FED. RULES OF CRIMINAL PROCEDURE FINAL REPORT 4 (Nov. 1943), available at http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ CR11-1943.pdf; [*112] H.R. Rep. No. 65-291, at 20 (1917). Substantively, *Rule 41* mirrors, and in no way alters or expands, the *Fourth Amendment*. *Rule 41* is not the font of *Fourth Amendment* law; it is the codified expression of *Fourth Amendment* law.

Rule 41 generally governs all searches and seizures, but by its terms does not override other statutes that govern searches and seizures related to specific government investigation schemes, such as searches and seizures related to customs duties. *FED. R. CRIM. P. 41(a)(1)* (noting that *Rule 41* "does not modify any statute regulating search or seizure, or the issuance and execution of a search warrant in special circumstances"); *FED. R. CRIM. P. 41* Advisory Committee's Note, 1944 Adoption, Note to Subdivision (g) ("While *Rule 41* supersedes the general provisions of 18 U.S.C. . . . relating to search warrants, it does not supersede, but preserves, all other statutory provisions permitting searches and seizures in specific situations.").

Thus, where another statute specifically governs a search, seizure, or issuance and execution of a search warrant in special circumstances, *Rule 41* yields to all substantive provisions of that statute. See, e.g., *United States v. Berkos, 543 F.3d 392, 398 n.6 (7th Cir. 2008)* [*113] (holding that *Rule 41(a)(1)* excuses from compliance with *Rule 41* all other statutes that govern warrants, including *18 U.S.C. ß 2703(a)*, which creates a statutory "special circumstance" under *Rule 41(a)(1)* since "warrants pursuant to *ß 2703(a)* do not directly infringe upon the personal privacy of an individual, but instead compel a service provider to divulge records maintained by the provider for the subscriber."); *United States v. Kernell, Crim. No. 08-142, 2010 U.S. Dist. LEXIS 32802, 2010 WL 1408437, at *2-3 (E.D. Tenn. Apr. 2, 2010)* (holding that *ß 2703(a)*'s regulation of the search and seizure of electronic evidence rendered the substance of *Rule 41* inapplicable); *In the Matter of the Search of Yahoo, Inc., Crim. No. 07-3194, 2007 U.S. Dist. LEXIS 37601, 2007 WL 1539971, at *7 (D. Ariz. May 21, 2007)* (same). However, the government wisely does not argue that any applicable statute removes this matter from the purview of *Rule 41*. Moreover, the Court has been presented with no argument that *Rule 41(c)(2)* or *(3)* applies, and will therefore discuss only the provisions that are relevant to this case; namely, *Rule 41(c)(1)* and *(4)*. The government does not argue entitlement to the warrant under *Rule 41(f)* (warrant for tracking device). As [*114] discussed infra, the Court rules that the procedures of *Rule 41(f)* govern any request for prospective or real-time location data. However, *Rule 41(f)* could not and does not authorize issuance of a warrant beyond the constitutionally permissible categories or purposes set forth in *Rule 41(c)(1)-(4)*.

a. *Rule 41(c)(1)*

Rule 41(c)(1) requires, as does the *Fourth Amendment*, that the government establish probable cause that its search for information be narrowly tailored to reveal "evidence of a crime." See *FED. R. CRIM. P. 41(c)(1)*. A defendant's ongoing location or his pattern of travel can constitute "evidence of a crime" sufficient to meet *Rule 41(c)(1)* when, for example, he is suspected of involvement in a drug trafficking crime. See, e.g., *Garcia-Villalba, 585 F.3d at 1234* (recognizing that a defendant's physical movements from place to place established sufficient nexus); *Rojas, 671 F.2d at 165 n.8* ("[W]arrants are issued for surveillance or tracking devices on probable cause that the 'search' (the

surveillance or tracking) will uncover evidence of a crime . . ."); In re Application of the United States . . ., Misc. No. 06-186, 187, 188, 2006 WL 6217584, at *4 n.6 (D.D.C. Aug. 25, 2006) [*115] ("Cell site and geolocation information may be evidence of a crime because, for example, a subject's location can be used to rebut an alibi or place him at the scene of a crime. Here, the location of a suspect known to be purchasing narcotics, or of one known to be guarding and selling a large quantity of narcotics, is likely to reveal the location of the drug stash house."). Thus, a *Rule 41(c)(1)* search warrant for location information may properly issue where there is a clear nexus between the location data sought and the crime.

The government initially alleged, without any supporting facts, that the defendant was a "fugitive," but withdrew that assertion at the hearing. (ECF No. 15, 17-18). Although the government no longer contends the subject was a "fugitive," it is important to note that an unsupported allegation of fugitive status does not alone constitute justification for a warrant. See *In re Application for the Installation and Use of a Pen Register, 439 F.Supp. 2d 456, (D. Md. 2006)* (rejecting the Government's application for cell site information under the Pen/Trap Statute and *18 U.S.C. ß 2703(d)* in connection with the criminal investigation of a fugitive from justice wanted [*116] for unlawful flight to avoid prosecution under *18 U.S.C. ß 1073*, but stating that the Court "would immediately issue a warrant under *Rule 41, Fed. R. Crim. P.*, if the government provided a sworn affidavit attesting to the facts of the application," including that defendant had placed calls from the subject cellular telephone since becoming a fugitive). Rather, the government must demonstrate that the defendant fled the state with the intent of avoiding prosecution, thus engaging in action that would constitute a chargeable crime that would provide the requisite predicate for a search warrant under *Rule 41(c)(1)*. See *18 U.S.C. ß 1073* ("[W]hoever moves or travels in interstate or foreign commerce with intent to either (1) to avoid prosecution, or custody or confinement after conviction, under the laws of the place from which he flees . . ."). Importantly, the defendant must first meet the definition of "fugitive," which the Fourth Circuit has carefully articulated as a "person who has fled to avoid prosecution for [a] crime." *United States v. Spillane, 913 F.2d 1079, 1083-84 (4th Cir. 1990)*.

Although some courts have declined to apply the seldom-prosecuted *ß 1073* to fugitive federal defendants, [*117] see, e.g., *United States v. Noone, 938 F.2d 334, 334-37 (1st Cir. 1991)*, few have had occasion to interpret the statute, *United States v. McKinney, 785 F. Supp. 1214, 1218 (D. Md. 1992)*. This Court and the Fourth Circuit have, however, read *ß 1073* to cover federal defendants. See, e.g., *United States v. Rohn, 964 F.2d 310, 312-13 (4th Cir. 1992)* (recognizing without criticism the district court's jury instruction that a defendant's unauthorized flight with intent to avoid prosecution constituted a violation of federal law under *18 U.S.C. ß 1073* where defendant was charged with document fraud under federal statutes); *United States v. Davis, 233 Fed. Appx. 292, 294 (4th Cir. 2007)* (upholding as reasonable a defendant's sentence for multiple federal crimes including violation of *18 U.S.C. ß 1073* for conspiracy to commit flight to avoid prosecution); *United States v. X, 601 F. Supp. 1039, 1041 (D. Md. 1984)* (discussing the option of a *ß 1073* charge against a federal defendant); *United States v. Y, 601 F. Supp. 1038, 1039 (D. Md. 1983)* (same); *United States v. Walters, 558 F. Supp. 726, 730 (D. Md. 1980)* (same). Thus, where there is evidence of flight from prosecution, the government can [*118] obtain the type of location data sought here, as his location would then be evidence of a crime. As discussed below, courts have granted orders for location data or other extraordinary surveillance under the All Writs Act to aid in the apprehension of a defendant where flight is shown. This avenue would assist law

enforcement in its apprehension of criminal defendants while assuring the detached review of a judicial officer in the salutary procedural framework of the Federal Rules of Criminal Procedure.

However, where, as here, a defendant is charged with a discrete crime that is not continuing in nature and that would not result in the defendant's likely possession of tangible or intangible items related to his commission of that crime, *Rule 41(c)(1)* does not authorize a search warrant. See, e.g., *Walters, 558 F. Supp. at 730* (finding that, "[u]nless the government can, pursuant to some criminal statute such as *18 U.S.C. ß 1073* (Flight to Avoid Prosecution or Giving Testimony), show probable cause to believe that defendant used or is using [his] phones in furtherance of a federal offense, such as flight to avoid apprehension, it does not appear that this Court has the authority under [*119] *Rule 41(b)(3)* to order the production of the telephone records" requested under the Wiretap Act); *United States v. X, 601 F. Supp. 1039, 1041 (D. Md. 1984)* (same). Therefore, just as the government failed to meet its burden under the *Fourth Amendment*, its request does not satisfy *Rule 41(c)(1)*.

b. *Rule 41(c)(4)*

Rule 41(c)(4) permits issuance of a warrant supported by probable cause that the search will reveal "a person to be arrested or a person who is unlawfully restrained." *FED. R. CRIM. P. 41(c)(4)*. Although the government admits that its search in this case would not reveal a literal person, it nonetheless suggests that its request for location data "properly falls within the scope of a search for a person to be arrested," if the Court accepts a broad construction of the Rule. (ECF No. 10, 5). The Court acknowledges the at least superficial logic of this expanded reading. However, having found that the *Fourth Amendment* does not sanction issuance of a warrant under these circumstances and having further concluded that *Rule 41* must be read consistently with the *Fourth Amendment*, reliance on *Rule 41(c)(4)* does not advance the government's case. Moreover, the government has not identified [*120] any language in the rule, its legislative history, or case law that aids its position. Thus, the Court declines to adopt the government's expansive reading of *Rule 41(c)(4)* in the context of the warrant application at issue in this matter.

As discussed earlier in section (1)(d), the rule was changed because in 1979 "there was uncertainty whether a warrant was needed to enter a private premises to make an arrest." 3A FEDERAL PRACTICE & PROCEDURE, CRIM. ß664.1 (3d ed. 2009).

The notes of the Advisory Committee on the Federal Rules of Criminal Procedure's rationale for amending *Rule 41* to include *subsection (c)(4)* in 1979 are additionally informative:

> This amendment to *Rule 41* is intended to make it possible for a search warrant to issue to search for a person under two circumstances: (i) when there is probable cause to arrest that person; or (ii) when that person is being unlawfully restrained. There may be instances in which a search warrant would be required to conduct a search in either of these circumstances. Even when a search warrant would not be required to enter a place to search for a person, a procedure for obtaining a warrant should be available so that law enforcement officers [*121] will be encouraged to resort to the preferred alternative of acquiring "an objective predetermination of probable cause," *Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)*, in this instance, that the person sought is at the place to be searched."

FED. R. CRIM. P. 41(c)(4), Advisory Committee's Note, 1979 Adoption.

Thus, this amendment to *Rule 41* was clearly not intended to be a break from the requirement of probable cause to believe that the subject of the search is in a particular place. Rather, the amendment provided a procedure for law enforcement to present its case to a "neutral magistrate" for search of a particular location while protecting the privacy rights of third parties.

The Fifth Circuit, interpreting the Advisory Committee Notes, found that

> [T]he provision was intended to cover two distinct situations not applicable to the case at hand: (1) where an individual for whom probable cause for arrest exists, but is "hiding out" with someone else; and (2) in searching for a kidnap victim believed to be held captive in a given place.
>
> Given the narrow intent behind this rule, and the coverage of arrest warrants in *Fed. R. Crim. P. 4* and *9*, we do not read *Rule 41* to [*122] extend to arrest situations.

United States v. Hultgren, 713 F.2d 79, 85 n.9 (5th Cir. 1983). Although the 1979 Amendments to *Rule 41* took effect prior to the Supreme Court's ruling in Steagald v. United States, the rationale for *Rule 41(c)(4)* is consistent with the Steagald Court's holding just two years later that law enforcement must obtain a search warrant before entering a third-party residence to apprehend the subject of an arrest warrant to protect third party privacy interests. See *451 U.S. 204, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981)*. [22]

> 22 While later decisions in some circuits suggest that a warrant based on probable cause may not be necessary vis a vis the subject of the arrest warrant, see infra, it is still necessary to protect the interests of third parties.

Based on the foregoing analysis, the Court agrees that *Rule 41(c)(4)* authorizes the Court to issue a warrant to search for a person where there is probable cause to arrest the person and there is probable cause to believe that he is hiding in a particular place. *Walters, 558 F. Supp. at 730*; *FED. R. CRIM. P. 41(c)(4)*, Advisory Committee's Note, 1979 Adoption. There is no suggestion that this rule change was intended to empower the government to obtain [*123] the type of location data requested here, on the type of showing proffered here. The Court finds that *Rule 41(c)(4)* simply does not encompass a broad search for information as to the ongoing location of the subject of an arrest warrant (as opposed to a search of specific places for the defendant), where supported by nothing more than an arrest warrant and a belief that the subject of the arrest warrant possesses a cell phone.

In sum, under the federal rules it is proper for the government to get a search warrant for evidence of a crime including, for example, location data pertaining to a suspected drug dealer. See *FED. R. CRIM. P. 41(c)(1)*. In addition, it is proper for the government to get a warrant to search for the subject of an arrest warrant where it can demonstrate probable cause to believe that the subject of the arrest warrant is in a particular place. See *FED. R. CRIM. P. 41(c)(4)*. Notwithstanding, there seems to be no authority supporting the issuance of a search warrant to obtain information about the location of the subject of an arrest warrant solely to aid in that person's apprehension under the rubric of *Rule 41(c)(1)-(4)*. However, as discussed below, the government's [*124] application is,

in fact, a request for a tracking device, which necessarily must be considered under *Fed. R. Cr. P. 41(f)(2)*. This rule quite obviously does not indicate that the showing necessary for issuance of a tracking device warrant is any different than required under *Fed. R. Cr. P. 41(c)(1)-(4)*; however, it does establish distinct and definite procedures for tracking warrants. Accordingly, neither *41(c)* nor *41(f)* provides any support for the government's view of the permissibility of a warrant for tracking or location data on the showing it proffers.

3. Inherent Authority

The government also argues that a federal court retains inherent authority to issue warrants consistent with the *Fourth Amendment*, without regard to the terms of *Rule 41*. (ECF No. 6, 4). [23]

> 23 The government is correct that there is nothing in *Rule 41* which expressly prohibits a warrant for the information sought. In that sense, the government's request is not inconsistent with *Rule 41*; nor, of course, does *Rule 41* expressly provide authority for issuance of the warrant or order it seeks. But this, of course, is the wrong focus. *Rule 41* does not define the limits of constitutional permissibility. The *Fourth Amendment* [*125] does.

The Federal Public Defender does not deny that the federal court has inherent authority to issue search warrants. (ECF No. 8, 1-2). However, the Court can only issue warrants which comply with the *Fourth Amendment* and, as discussed above, warrant authority has historically been jealously limited to use in connection with criminal conduct. None of the government's authorities in support of the exercise of inherent authority here represent a deviation from this overwhelming, historical and precedential view of the permissible use of a search warrant. See (ECF No. 6, 4-6).

The government relies heavily on *United States v. N.Y. Telephone Co., 434 U.S. 159, 98 S. Ct. 364, 54 L. Ed. 2d 376 (1977)*, for its position. Although N.Y. Telephone Co. interpreted *Rule 41(c)* broadly to include electronic intrusions, namely pen registers, the decision provides no support on the pivotal issue here. In that case, the Supreme Court held that the district court had the power to order the installation of the pen registers to search property that was being used as the means to commit a criminal offense, that is, a "telephone suspected of being employed as a means of facilitating a criminal venture." *Id. at 169*. Thus, N.Y. Telephone [*126] Co. expands the type of evidence of a crime for which a warrant may issue; it does not endorse issuance of a search warrant for the new and different purpose of obtaining information to aid in the apprehension of a criminal defendant. Accord *United States v. Southwestern Bell Telephone Co., 546 F.2d 243, 245 (8th Cir. 1976)* (same).

The government's other authorities are similarly distinguishable. The courts in *United States v. Torres, 751 F.2d 875 (7th Cir. 1984)*, *United States v. Villegas, 899 F.2d 1324 (2nd Cir. 1990)*, and *United States v. Falls, 34 F.3d 674, 678 (8th Cir. 1994)*, approved, respectively, video surveillance in a terrorism investigation, photographs without seizure of any tangible items in the course of an investigation of drug conspiracy, and silent video in a drug trafficking investigation. This Court agrees with the Eighth Circuit in Southwestern Bell Telephone Co. that "[t]he unusual character and technological advances of electronic communications have occasioned the surfacing of this inherent authority [outside of *Rule 41*]." *546 F.2d at 245 n.5*. However, while that proposition is certainly true insofar as law enforcement must be able to use evolving and up-to-date [*127] technology in evidence gathering of criminal conduct, it does not follow that new technology can be used for a

purpose not sanctioned in the *Fourth Amendment* warrant clause. None of the government's authority supports its view of the *Fourth Amendment*.

4. The Stored Communications Act, (*18 U.S.C. ß 2703(c)(1)(A)*)

The government's first application sought a search warrant under the combined authority of *Rule 41* and *18 U.S.C. ß 2703(c)(1)(A)*. Specifically, the government alleges that *18 U.S.C. ß 2703(c)(1)(A)*, a provision enacted as part of the Electronic Communications Privacy Act of 1986, entitles it to a warrant for the requested information. (ECF No. 10, 5-6). *Section 2703(c)(1)(A) of Title 18* provides that "[a] governmental entity may require a provider of electronic communication . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) when it obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure." *18 U.S.C. ß 2703(c)(1)(A)*. The government argues based upon this statutory language that this Court has

> jurisdiction to issue a search warrant here [*128] . . . because (1) the telecommunications service provider is a provider of electronic communication service; (2) the location information sought pertains to a customer of the service; and (3) the location information sought is not the contents of communications. *Section 2703(c)(1)(A)* thus constitutes an explicit statutory authorization for the United States to obtain the location information it sought in this case"

(ECF No. 10, 5-6) (internal citations omitted). The government's argument fails as a matter of constitutional law and a matter of statutory interpretation. A brief review of the legislation on electronic communications and records is helpful to understanding the fallacy of the government's argument here.

In 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act to provide comprehensive authorization for government interception, under carefully subscribed circumstances, of wire or oral conversations. S. Rep. No. 99-541, reprinted in 1986 U.S.C.C.A.N. 3555, 3556 (Oct. 17, 1986) (citing the Omnibus Crime Control and Safe Streets Act of 1968). This Act, which included Title III's wiretap provisions, quickly became "hopelessly out of date." Id. In 1986, Congress [*129] enacted the Electronic Communications Privacy Act ("ECPA") which amended Title 18 of the United States Code to "protect against unauthorized interception of electronic communications," and to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." Pub. L. No. 99-508, 100 Stat. 1848 (99th Cong. 1986); S. Rep. No. 99-541, reprinted in 1986 U.S.C.C.A.N. 3555, 3555 (Oct. 17, 1986). Of particular note, ECPA amended Title III to "bring it in line with technological developments and changes in the structure of the telecommunications industry," and added sections to address access to stored wire and electronic communications and transactional records, as well as pen registers and trap and trace devices. Id. [24]

24 When reporting ECPA, the Senate underscored the important purpose of this legislation:

> A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case law,

> and U.S. Postal Service statutes and regulations. Voice communications transmitted via common carrier are protected by title III of the Omnibus Crime Control [*130] and Safe Streets Act of 1968. But there are no comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new forms of telecommunications and computer technology. This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.
>
> This gap results in legal uncertainty. It may unnecessarily discourage potential customers from using innovative communications systems. It probably encourages unauthorized users to obtain access to communications to which they are not a party. It may discourage American businesses from developing new innovative forms of telecommunications and computer technology. The lack of clear standards may expose law enforcement officers to liability and may endanger the admissibility of evidence.
>
> **Most importantly, the law must advance with the technology to ensure the continued vitality of the *fourth amendment*. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to** [*131] **protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.**

Id. at 3559 (emphasis added).

Following adoption of the ECPA, courts have recognized that,

> there are four broad categories of electronic surveillance, each with its own well-established standard for obtaining court ordered disclosure or monitoring. Those categories (arranged from highest to lowest order of legal process) are: **(1) wiretaps**, which are authorized pursuant to *18 U.S.C. ßß 2510-2522*, upon what could be called a "probable cause plus" showing; **(2) tracking devices**, which are authorized pursuant to *18 U.S.C. ß 3117*, upon a standard probable cause showing; **(3) stored communications and subscriber records**, which are authorized pursuant to the Stored Communications Act upon a showing of specific and articulable facts showing that there are reasonable grounds to believe that the data sought is relevant and material to an ongoing criminal investigation; [25] and **(4) pen registers and trap and trace devices**, which are authorized pursuant to *18 U.S.C. ßß 3121-3127* . . . upon the Government's certification that the data sought is relevant to an ongoing criminal investigation. [26]

In re Application of the United States . . ., Misc. No. 06-186, 187, 188, 2006 WL 6217584, at *2 (D.D.C. Aug. 25, 2006) [*132] (citing *In re Application for Pen Register. . ., 396 F. Supp. 2d at 753*). ECPA defined "tracking devices," which it then explicitly excluded from coverage under the Act. *18 U.S.C. ßß 2510*, *3117*.

25 The Third Circuit has held that a magistrate judge has discretion to require a warrant with its underlying probable cause standard, rather than a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought . . . [is] relevant and material to an ongoing criminal investigation," before granting an order under *ß 2703(d)* of the Stored Communications Act. In re United States..., *620 F.3d 304, 319 (3d Cir. 2010)*.

26 While this opinion mentions Title 18's pen register and trap and trace provisions in the context of the "hybrid theory" proposed by the government and accepted by some courts for provision of cell site location information, these provisions are irrelevant to the precise location information requested herein, as the provisions are limited to "dialing, routing, addressing, and signaling information utilized [*133] in the processing and transmitting of wire or electronic communications." *18 U.S.C. ß 3121(c)*. While the pen/trap provision could arguably be read, as some courts have done, to include stored cell site location information as "call identifying information," e.g., In re Application of the United States . . ., 06-MC-6 & 06-MC-7, 2006 WL 1876847 (N.D. Ind. 2006); *In re Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wisc. 2006)*, the majority approach holds that location information is expressly exempted from these provisions by CALEA. E.g., *In re Application for Pen Register. . ., 396 F. Supp. 2d at 757-58*; *47 U.S.C. ß 1002(a)(2)*. However, because the information sought in this case is precise location information that cannot be classified as call identifying information in the first place, the Court need not reach this issue.

The Wiretap Act and ECPA apply only to the extent information is transferred via wire, oral, or electronic communication. Thus, these Acts now go beyond protecting only wire or oral communication to also cover any electronic communication, which includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in [*134] whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." *18 U.S.C. ß 2510(12)*. Thus, the electronic communications category covers cellular telephone service. *In re Application of the United States . . ., 405 F. Supp. 2d at 445*. [27]

27 The Wiretap Act establishes a higher standard for the "contents" of contemporaneous electronic communications, as opposed to "records concerning" the communication. Compare *18 U.S.C. ß 2703(c)-(d)* (permitting a governmental entity to obtain records or other information concerning electronic communications, not including the contents thereof, upon a warrant issued under *Rule 41* that meets the probable cause standard) with *18 U.S.C. ß 2518* (permitting a governmental entity to intercept electronic communications only after meeting a heightened probable cause standard). However, neither party contends that the precise location information sought by the government here is "contents" of an electronic communication that would fall within the Wiretap Act's protections against interception. Therefore, it is unnecessary for the Court here to analyze the intricacies and protections of [*135] the Wiretap Act.

The government contends that the information it seeks constitutes "records or other information pertaining to a subscriber" that it may request from a carrier by obtaining a warrant under *ß 2703(c)(1)(A)*. The statute offers no definition nor explanation of what constitutes "records" or "information pertaining to a subscriber."

The kind of location information that is most commonly sought under *ß 2703* is cell site data - information that is automatically collected by cell sites as a user's handset "checks in" or "registers" with the network. [28] 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 [*136] 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. ßß 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.

28 When requesting cell site information, the government often advances a "hybrid" theory using the combined authority of *18 U.S.C. ßß 2703(d) & 3121, et seq.*, which it contends allows it to obtain cell site location data without establishing probable cause. (ECF No. 1, 2 n.1). As explained by Judge Hogan of the D.C. District Court,

> The "hybrid theory" posits that the Court is authorized to order the disclosure of prospective cell site data under a combination of the [Stored Communications Act] and the Pen Register Statute. The government argues that the use of the word "solely" necessarily implies that [*137] another authority may be combined with the Pen Register Statute to authorize disclosure. Most of the Magistrate Judges that have considered the hybrid theory have found it to be unavailing, holding that the Pen Register Statute and the Stored Communications Act in tandem do not provide authority for disclosure of prospective cell site data. The first District Court to rule on the hybrid theory, however, has come out the other way, finding that this combination does allow for disclosure.

In re Application of the United States . . ., Misc. No. 06-186, 187, & 188, 2006 WL 6217584, at *2 (D.D.C. Aug. 25, 2006). Judge Hogan followed the majority of courts in rejecting this theory and concluding instead that "prospective cell site and geolocation information is available upon a traditional probable cause showing under *Rule 41*." *Id. at *3*. Again, however, this particular theory is not implicated here, and the Court need not now pass judgment on the heavily criticized approach.

At the hearing, the government admitted that the precise location data sought here is neither ancillary information collected by service providers in the course of business nor information that is automatically generated [*138] or stored "incidental" to calls. Therefore, the requested information cannot logically be considered "records" and is nothing like the information courts have found to fall under the purview of *ß 2703*. (ECF No. 10, 5). Regardless of the Court's view of this argument, the argument is at best merely semantic. To the extent *ß 2703* applies to a search of an area or thing that is entitled to a reasonable expectation of privacy, the *Fourth Amendment* protects. To the extent

Rule 41 contains substantive provisions, that substance is rooted directly in the *Fourth Amendment*, with which any search that would violate a reasonable expectation of privacy must comply. As the Federal Public Defender noted, "[t]he government's reference to *ß 2703(c)(1)(A)* adds nothing to the analysis of this issue." (ECF No. 8, 11). The Court agrees.

Rather than being a "stored record or other information," the precise location information sought falls squarely within the definition of communications from a tracking device, despite the government's denial of the same in this case. *18 U.S.C. ß 3117* defines a tracking device as "an electronic or mechanical device which permits the tracking of the movement of a person [*139] or thing." As such, the information is specifically excluded from coverage under the Wiretap Act and ECPA, including *ß 2703*. [29] *18 U.S.C. ßß 2510(12)(C)*, *3117(b)*. Thus, the government's argument fails as a matter of straightforward statutory interpretation. [30]

29 Two bills, part of the previously mentioned proposed legislation to update ECPA, strengthen the arguments that ECPA does not cover location data--rather, location data stands separate from other types of data covered by the Act. Senator Leahy's ECPA Amendments Act of 2011, "Leahy Bill," adds "geolocation information," defined as "any information concerning the location of an electronic communications device that is in whole or in part generated by or derived from the operation or use of the electronic communications device" under the coverage of the Act, and further defines "electronic communications device" to mean "any device that enables access to or use of an electronic communications system, electronic communication service, remote computing service, or geolocation information service." S. 1011, 112th Cong. (2011). Alternatively, Senator Wyden and Representative Chaffetz's the Geolocational Privacy and Surveillance Act, "Wyden [*140] Bill," provides for geolocation information by supplementing ECPA. The bill defines "geolocation information" as any information "that is not the content of a communication, concerning the location of a wireless communication device or tracking device [defined as an electronic or mechanical device which permits the tracking of the movement of a person or object] ... that, in whole or in part, is generated by or derived from the operation of that device and that could be used to determine or infer information regarding the location of the person." H.R. 2168, 112th Cong. (2011). The bill's rules are modeled after the federal wiretapping statute, *18 USC ß 2511*. Wyden, Chaffetz Introduce Geolocation Privacy and Surveillance ("GPS") Act, http://wyden.senate.gov/issues/issue/?id=b29a3450-f722-4571-96f0-83c8ededc332#sections (last visited Jul. 21, 2011). Both bills and their definitions of geolocation data support that the information the government seeks would be covered by ECPA only if it were amended or supplemented.

30 Given that *ß 2703* does not provide authority for law enforcement access to location data under the circumstances presented here, the government's novel argument that a *ß 2703* [*141] warrant need not comply with *Rule 41* in its entirety, but rather only with procedural provisions in the Rule, is inapposite. See (ECF No. 10, 5) (arguing that its warrant application need not correspond to the categories listed in *Rule 41(c)(1)-(4)*). The government maintains that the provision in *ß 2703(c)(1)(A)* authorizing it to obtain "information pertaining to a subscriber or customer" from an electronic communication service pursuant to "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure," indicates that *ß 2703* incorporates only those provisions of *Rule 41* that are procedural in nature, not its substantive provisions. (Id.) (citing *Berkos, 543 F.3d at 398*). The government cites several unreported district court cases finding that a *ß 2703* warrant does not incorporate the

provisions of *Rule 41(b)* pertaining to authority to issue a warrant, and argues that, like *Rule 41(b)*, the provisions of *Rule 41(c)* are properly categorized as substantive. (Id.) (citing *Kernell, 2010 U.S. Dist. LEXIS 32802, 2010 WL 1408437, at *4 (E.D. Tenn., Apr. 2, 2010)*; *In re Search of Yahoo, Inc., 2007 U.S. Dist. LEXIS 37601, 2007 WL 1539971, at *7 (D. Ariz., May 21, 2007)*Therefore, the government argues that the items seized [*142] pursuant to a warrant issued under *ß 2703(c)(1)(A)* need not comply with the itemized categories of *Rule 41(c)*. However, as the Court has set forth above, *ß 2703* does not apply to the location data requested in the underlying applications. The allowable purposes of a search warrant are defined by constitutional law; the *Fourth Amendment* trumps any statutory argument..

b. Tracking Devices

The government's position, as articulated during the hearing, is that a cell phone is not a tracking device. Rather, the government contends that the tracking devices contemplated by ECPA and *Rule 41* include only the legacy "bumper beepers" that existed at the time Congress enacted ECPA. The Court disagrees.

When Congress enacted ECPA in 1986, it had no reason to anticipate that cell phones would soon become capable of performing all the functions of a tracking device. Nonetheless, instead of limiting its statutory definition of tracking device to the beeper-type devices then in existence, it defined a tracking device broadly as "an electronic or mechanical device which permits the tracking of the movement of a person or object." *18 U.S.C. ß 3117(b)*. In the Senate Report that accompanied ECPA, the only [*143] reference to tracking devices defined "electronic tracking devices" as:

> one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such "homing" devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.

S. Rep. No. 99-541, reprinted in 1986 U.S.C.C.A.N. at 3564.

Only a single court, in an unreported opinion, has agreed with the government's position that Congress intended to limit "tracking devices" to include only traditional beeper-type tracking devices. *In re Application for an Order Authorizing The Extension and Use of a Pen Register . . ., 2007 U.S. Dist. LEXIS 11692, 2007 WL 397129, at *2 (E.D. Cal. Feb. 1, 2007)* (commenting that "it would prove far too much to find that Congress contemplated legislating about cell phones as tracking devices"). The more prevalent view among courts is that the statute is not so limited. This Court agrees with the Southern District of Texas's thoughtfully articulated conclusion that the broad [*144] definition of tracking devices adopted by Congress was intended to encompass not only the limited beeper-type device that existed at the time, but also future technological permutations of tracking devices. See *In re Application for Pen Register . . ., 396 F. Supp. 2d at 754-55*.

Other arguments that cell phones are not tracking devices when used to effectively track a subject are similarly unavailing. For instance, some suggest that tracking devices covered by the statute should be limited only to devices which are "installed" or "planted" without the subject's

consent or knowledge. *In re Application for Pen Register . . ., 2007 U.S. Dist. LEXIS 11692, 2007 WL 397129, at *2*; *In re Application of the United States . . ., 411 F. Supp. 2d 678, 681 (W.D. La. 2006)*. However, the statute contains no such requirement. The suggestion that "[i]f the owner of a cell phone does not wish to convey [his location data], he can simply not make a call or he can turn his cell phone off," is similarly inaccurate. Id. When a cell phone is turned on and located within its network, it is constantly registering its current location with the nearest cell tower. See CTIA-The Wireless Association, Wireless Glossary of Terms, available [*145] at http://www.ctia.org/media/industry_info/index.cfm/AID/10321. While the government can limit its request to cell site data recorded only at the origination and termination of calls, e.g., while the phone is actively being used, it can also request that the carrier collect this registration information at any time while the phone is powered on without the user's knowledge or consent. Precise location data can also be generated independently of calls, at the request of the carrier, and without the user's knowledge or consent, as was requested here.

The majority of courts that have examined these issues are now recognizing that advances in technology have transformed cell phones into multi-function devices that perform, in many cases, identical functions to traditional tracking devices. The logical approach embraced by these courts concludes that cell phone signals are electronic communications and cell phone providers are electronic communications service providers, except to the extent that a cell phone is being used as a tracking device, e.g., to provide location data. E.g., In re Application of the United States . . ., 2009 WL 159187 (S.D.N.Y. Jan. 13, 2009); United States v. Bermudez, IP05-0043-CR05-BF, 2006 WL 3197181, at *9-10 (S.D. Ind. Jun. 30, 2006); [*146] *In re Application of the United States . . ., 402 F. Supp. 2d at 604*; *In re Application of the United States . . ., 384 F. Supp. 2d 562, 563-64 (E.D.N.Y. 2005)*. In reaching this conclusion, these courts have found that,

> [a] cell phone has the ability, by the use of electronic signals, to track the movement of an object (the phone itself), and by extension, of a person. It does so by locating the position of the phone, through the process of "triangulation" that Judge Kaplan and others discuss at some length in their opinions. Therefore, a cell phone falls within the literal definition of the term "tracking device" as used in the Stored Communications Act.

In re Application of the United States . . ., 2009 WL 159187, at *3 (Jan. 13, 2009). See also Bermudez, IP05-0043-CR05-BF, 2006 WL 3197181, at *9-10; *In re Application of the United States . . ., 402 F. Supp. 2d at 604*; *In re Application of the United States . . ., 384 F. Supp. 2d at 563-64*.

This judge now joins others who have found that cell phones, to the extent that they provide prospective, real time location information, regardless of the specificity of that [*147] location information, [31] are tracking devices. Thus, a cell phone's prospective, real time location data [32] -- whether cell site or GPS -- is a communication from a tracking device that is excluded from coverage under the Wiretap Act and ECPA. As noted by the Southern District of New York,

> [t]his is an elegant solution to the conundrum created by the application of Congress' chosen definitions. It construes the statute in a way that makes it work in the manner that Congress clearly intended, without doing violence to its literal language. It avoids

> the absurd result that has caused some of my fellow jurists to dance around the Congressionally-selected definitions of the terms "tracking device" and "electronic communication." And it quite possibly forestalls any *Fourth Amendment* issue that might arise from the use of [cell site location data] in violation of the Supreme Court's pronouncement in *United States v. Karo, 468 U.S. 705, 714, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984)*.

In re Application of the United States . . ., 2009 WL 159187, at *5 (S.D.N.Y. Jan. 13, 2009). This conclusion does not prohibit the government from obtaining prospective, real time data. [33] Rather, such information may be obtained in the same way that [*148] the government may obtain information from a tracking device: by meeting the requirements of *Rule 41* and the *Fourth Amendment*.

> 31 In other cases, the government has suggested that only precise location information from cell phones should be categorized as tracking information, and that category should be distinguished from prospective and real-time cell site location information. However, *ß 3117* does not distinguish between general and detailed tracking, and courts have rejected such a distinction. See *In re U.S. for Orders Authorizing Use of Pen Registers. . . , 416 F. Supp. 2d 390, 395-96 & n.9 (D. Md. 2006)* (commenting that the court is not convinced by the government's argument that provision of general cell site information does not convert a cell phone into a tracking device, and stating that "[t]he definition of "tracking device" is broad and contains no articulation of how precise a device must be"); *In re Application for Pen Register. . ., 396 F. Supp. 2d at 755-56 (S.D. Tex. 2005)* (finding that the fact that cell phone location information may not be as detailed or accurate as a traditional tracking device is irrelevant, as the statute does not distinguish between general and [*149] detailed tracking).
> 32 Unlike historical location information, prospective location information includes any location information generated after the date of the Court order that permits the government to obtain that information. Real time location information, a subset of prospective location information, includes only information that is both generated after the Court's order and is provided to the government in, or close to, "real time."
> 33 Moreover, contrary to the conclusion of the Eastern District of New York, this Court does not find that classification of cell phones as tracking devices to the extent they act as tracking devices does not render *ß 2703(c)* meaningless. Cf. *In re U.S. for an Order Authorizing the Use of Two Pen Register . . ., 632 F. Supp. 2d 202, 207-08 (E.D.N.Y. 2008)* (adopting the hybrid theory and declining to classify a cell phone as a tracking device as, in its opinion, to do so would result in a carrier having "no obligation to disclose any information to the government under *Section 2703(c)*"). Indeed, as other courts have alluded, the government may still obtain historical location information as well as numerous other categories of stored information under [*150] *ß 2703(c)*. See, e.g., *In re U.S. for an Order Authorizing the Use of Two Pen Register . . ., 632 F. Supp. 2d 202, 207-08 (E.D.N.Y. 2008)*; *In re Application of the United States . . ., 405 F. Supp. 2d at 447* (authorizing single tower, call-related information request when the government utilized a *2703(c)* theory).

The Court recognizes that there is some dispute as to whether a warrant based on probable cause is required in obtaining the traditional "bumper beeper." The Supreme Court on June 27, 2011 granted the government's petition for certiorari in *United States v. Jones, 625 F.3d 766, 393 U.S.*

App. D.C. 194 (D.C. Cir. 2010), a companion case to *United States v. Maynard, 615 F.3d 544, 392 U.S. App. D.C. 291 (D.C. Cir. 2010)*, discussed supra, presenting a *Fourth Amendment* challenge to warrantless GPS surveillance of automobiles. *United States v. Jones, 2011 U.S. LEXIS 4956, 2011 WL 1456728 (Jun. 27, 2011)* (granting certiorari). Accordingly, the Supreme Court is poised to address during the coming term: (1) whether the warrantless use of a tracking device on a defendant's vehicle to monitor its movements on public streets violates the *Fourth Amendment*; and (2) whether the government violated the defendant's *Fourth Amendment* rights by installing a GPS device [*151] on his vehicle without a valid warrant and without his consent. (Id.). Relevant to the instant matter, these issues implicate the questions of whether and under what circumstances continuous GPS surveillance constitutes a "search" under the *Fourth Amendment*, thereby necessitating probable cause and a warrant. While the Supreme Court's opinion in this case may be helpful, the intrusion of privacy implicated in cell phone tracking as discussed earlier is much more certain and extensive. The government seems to recognize this and did not seriously question that the location data was a "search."

Having already found that the information sought here is subject to a reasonable expectation of privacy, the Court further concludes the government must obtain a search warrant under *Rule 41(f)* to obtain location data and must establish probable cause. As *ß 2703* does not govern the information requested here and the government has failed to establish the grounds for a warrant, the government's application brought under *Rule 41* and *18 U.S.C. ß 2703(c)(1)(A)* is unavailing.

5. All Writs Act

The government's second application sought precise location information under the All Writs Act. (ECF No. 2; ECF [*152] No. 6, 6-9). This may be the most troubling position the government has taken in pursuit of this precise location data. Essentially, the government seeks an end run around constitutional and statutory law through invocation of the All Writs Act. As discussed above, the Constitution delineates the appropriate uses of a search warrant, *Rule 41* and ECPA provide the procedural guidance for law enforcement seeking tracking data. The All Writs Act gives "a federal court [] the power 'to issue such commands' as 'may be necessary or appropriate to effectuate and prevent the frustration of orders that it has previously issued." (ECF No. 6, 6). Therefore, the government suggests that the All Writs Act may be properly invoked wherever the government (1) has an active, valid arrest warrant; (2) has a reason to believe that the requested information will lead to the location of the subject of that arrest warrant; and (3) the government is not aware of the subject's precise location at the moment the warrant is requested. According to the government, nothing more - such as exhaustion of other means of surveillance or apprehension, or an absence of alternative authority - is necessary to trigger [*153] invocation of the All Writs Act. Rather, the government appears to see the All Writs Act as an alternative source of inherent authority, rather than a limited, residual one, equally constrained by the *Fourth Amendment*.

In support of its invocation of the All Writs Act, the government relies heavily on N.Y. Telephone Company, a case in which the United States Supreme Court found that an order requiring a phone company to provide assistance in furtherance of a properly issued pen register was authorized under the All Writs Act. *United States v. N.Y. Tel. Co., 434 U.S. 159, 98 S. Ct. 364, 54 L. Ed. 2d 376 (1977)*. After first finding that the pen register had been properly issued on a showing of probable cause, which included establishment of a nexus between use of the phone and suspected commission of an ongoing crime, the Court analyzed the district court's order, issued under the All Writs Act, requiring the telephone company to provide technical assistance to law

enforcement in furtherance of the pen register. *Id. at 171-77*. Recognizing that the Wiretap Act authorized such orders, the Court commented that "it would be remarkable if Congress thought it beyond the power of the federal courts to exercise, where required, [*154] a discretionary authority to order telephone companies to assist in the installation and operation of pen registers, which accomplish a far lesser invasion of privacy. . . . to prohibit the order challenged here would frustrate the clear indication by Congress that the pen register is a permissible law enforcement tool." *Id. at 177-78*.

Thus, N.Y. Telephone Company stands for the proposition that the All Writs Act enables the Court to, in the absence of other enabling authority, issue supplemental orders to effectuate valid orders or warrants issued under existing law, but only to the extent any supplemental order issued does not constitute an additional invasion of privacy. Notably, and critically different than this matter, the Supreme Court acknowledged and deferred to congressional approval of a pen register as a permissible law enforcement tool. Also notably, the government had satisfied the lower court that there was probable cause - a nexus between use of the phone for which the pen register was sought and suspected commission of an ongoing crime. N.Y. Telephone Company does not grant the Court an unbridled inherent power to infringe on an individual's privacy rights, outside [*155] of the governing structure of the *Fourth Amendment*. In fact, this Court has been unable to locate a single case in which access was granted to search or seize *Fourth Amendment*-protected information under the All Writs Act, without satisfying the probable cause standard.

Rather, the All Writs Act empowers courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." *28 U.S.C. ß 1651(a)*. The Act is intended to provide courts with the "instruments needed to perform their duty, as prescribed by the Congress and the Constitution," *Harris v. Nelson, 394 U.S. 286, 300, 89 S. Ct. 1082, 22 L. Ed. 2d 281 (1969)* (citing *Price v. Johnston, 334 U.S. 266, 282, 68 S. Ct. 1049, 92 L. Ed. 1356 (1948))*, so as "to process litigation to a just and equitable conclusion." *ITT Comm. Dev. Corp. v. Barton, 569 F.2d 1351, 1359 (4th Cir. 1978)*. This specifically includes the authority to use its equitable powers to resolve any issues in a case properly before it. Id.

Courts generally recognize this as a gap-filling measure to issue orders necessary "to achieve 'the rational ends of law.'" *N.Y. Tel. Co., 434 U.S. at 172* (quoting *Harris v. Nelson, 394 U.S. 286, 299, 89 S. Ct. 1082, 22 L. Ed. 2d 281 (1969))*. Consequently, courts [*156] issue such writs to "prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained." Id.; See also *Scardelletti v. Rinckwitz, 68 Fed. Appx. 472, 477 (4th Cir. 2003)* (quoting *Pa. Bureau of Corr. v. United States Marshals Serv., 474 U.S. 34, 40, 106 S. Ct. 355, 88 L. Ed. 2d 189 (1985)*; *Miller v. Brooks (In re Am. Honda Motor Co.), 315 F.3d 417, 438-39 (4th Cir. 2003)* (finding that invoking the All Writs Act to order an injunction was proper where necessary to prevent direct frustration of the district court's settlement approval order). The fact that a party may be assisted in its discharge of its rights or duties by the issuance of a writ is not a sufficient basis for the writ. *Barton, 569 F.2d at 1360* (overruling a district court's application of the All Writs Act to effectuate an order mandating deposit of funds into the court when that order would have no practical effect in advancing the court's jurisdiction). Indeed, the All Writs Act cannot be used to circumvent the safeguards set in place by existing law anywhere those safeguards prevent the requesting party's result.

Courts analyze four elements when determining whether to invoke the All Writs Act. First, courts [*157] determine whether any applicable federal law governs the request. Where other

federal law controls, the All Writs Act is inapplicable. See, e.g., *Denedo, 129 S. Ct. at 2227-28* (holding that "where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling"); *Clinton v. Goldsmith, 526 U.S. 529, 537, 119 S. Ct. 1538, 143 L. Ed. 2d 720 (1999)* (noting that the All Writs Act does "not generally . . . provide alternatives to other, adequate remedies at law"); *Application of the United States of America for an Order, 08-Misc.-0298, 2008 U.S. Dist. Lexis 45311, at *5 n.3 (E.D.N.Y. Jun. 9, 2008)* (holding that *Fed. R. Crim. P. 57* and the All Writs Act were inapplicable where there is other controlling authority); *In re Application for Pen Register. . ., 396 F. Supp. 2d at 325-27* (holding that the All Writs Act is applicable only when used to "fill a gap in an existing statutory regime," and not to "trump existing statutory law governing the use of investigative techniques"). The government boldly asserts that "*Rule 41* does not [] 'specifically address' the issuance of all search warrants." (ECF No. 10, 6). This assertion is entirely without support or merit. [*158] *Rule 41* establishes procedures for all search warrants not excepted by other statutes, including those for tracking devices, and provides a framework for the *Fourth Amendment* which expressly covers all searches into areas covered by a reasonable expectation of privacy as well as warrants required for such searches.

Second, if no federal law governs the requested authorization, courts determine whether there is any constitutional issue implicated by the proposed authorization. Courts have applied the All Writs Act to issue an authorization for assistance in effectuating an existing search warrant and arrest warrant where no *Fourth Amendment* privacy rights or other constitutional issues are implicated. See *United States v. X, 601 F. Supp. 1039, 1042-43 (D. Md. 1984)* (using the All Writs Act to authorize production of toll records finding no subscriber privacy interest in them); *United States v. Doe, 537 F. Supp. 838, 840 (E.D.N.Y. 1982)* (using the All Writs Act to authorize a production of toll records as subscriber has no legitimate expectation of privacy in them); *Application of the United States of America for an Order . . ., M. No. 03-89, 2003 U.S. Dist. LEXIS 15227, 2003 WL 22053105, at *2 (D. Md. Aug. 22, 2003)* [*159] (authorizing access to surveillance videotapes of the public areas of an apartment complex under the All Writs Act "as no reasonable expectation of privacy on part of tenants or their visitors to hallway").

The All Writs Act does not excuse the government from its burden of establishing probable cause where constitutionally protected information is requested. See *In re Application of the United States . . ., 396 F. Supp. at 326-27* (denying an application for real-time cell phone location data when the government submitted "specific and articulable facts" and holding that probable cause would be required to obtain such data). This Court has not located, and the parties have not provided, a single case in which access was granted to search or seize *Fourth Amendment*-protected information under the All Writs Act absent probable cause.

Where no law occupies the space and no constitutional issues are raised, courts move to the third step: determining whether a prior order of the Court exists that a further order will aid. For example, where a pen register that is properly issued by the Court upon a showing of probable cause would be frustrated by the government's inability to carry out the [*160] authorized search without assistance from the telephone company, the All Writs Act may authorize a secondary order to require the telephone company to provide technical assistance to the government. *N.Y. Tel. Co., 434 U.S. at 171-77*. See also *United States v. X, 601 F. Supp. at 1042-43* (ordering a telephone company to provide limited toll records where the government had a valid arrest warrant, but the subject of that warrant was evading arrest and the government established that the toll records would provide information about his current whereabouts).

Fourth, after meeting all previous steps, the government must show that "exceptional circumstances" justify invocation of the All Writs Act. Other less intrusive means, *Pa. Bureau of Corr., 474 U.S. at 44*, a showing that other means had been attempted and were unsuccessful, *United States v. X, 601 F. Supp. at 1043*, and the likelihood of success, id., are all factors to consider. For example, the Supreme Court refused to order the United States Marshals Service to transport and supervise a witness in a *Section 1983* action who was in state correctional custody to effectuate a prior habeas corpus order. See *Pa. Bureau of Corr., 474 U.S. at 43-44*. [*161] There, the order sought would not effectuate the habeas order because no "exceptional circumstances" were demonstrated that the state could not handle transporting the witness to the courthouse itself. *Id. at 43-44*. Exceptional circumstances existed, however, where a defendant had "disappeared," efforts to locate him had been unsuccessful, defendant was likely to use his phone to contact his family members, and records collected under a pen register would likely reveal information concerning the defendant's whereabouts. See *United States v. X, 601 F. Supp at 1042-43*; *Doe, 537 F. Supp. at 838, 840* (authorizing production of the toll records of the mother of the subject of an arrest warrant where the subject failed to appear and had attained fugitive status); *United States v. Hall, 583 F. Supp. 717, 722 (E.D. Va. 1984)* (authorizing provision of credit card records belonging to the previous girlfriend of a federal fugitive where the credit card was closely connected with underlying controversy and the location of fugitive). See also *Application of the United States of America for an Order . . ., 2003 U.S. Dist. LEXIS 15227, 2003 WL 22053105, at *3* (use of All Writs Act proper to obtain security videotapes where an [*162] arrest warrant had issued for defendant, agent stated that defendant had disappeared, efforts to locate defendant had been unsuccessful, and it was likely that access to security videotapes would provide information about defendant's whereabouts); *Denedo, 129 S. Ct. at 2227 n.2* (use of All Writs Act proper where a coram nobis [34] order would be ineffectual in correcting a prior order, i.e., a prior conviction, because the defendant had left the military and thus the military had no jurisdiction over him). Exceptional circumstances also exist where law enforcement would be entirely unable to obtain information that the court had authorized under a pen register, absent an order for the phone company's compliance. *N.Y. Tel. Co., 434 U.S. at 171-77*.

34 Coram nobis is an ancient writ designed to correct errors of fact. *Denedo, 129 S. Ct. at 2220* (quoting *United States v. Morgan, 346 U.S. 502, 507, 74 S. Ct. 247, 98 L. Ed. 248 (1954))*.

In short, the All Writs Act may authorize a search in furtherance of a prior order only where no other law applies, no *Fourth Amendment* right to privacy is implicated, and exceptional circumstances are present.

This is not such a situation. Here, the government requests information that implicates [*163] the *Fourth Amendment's* reasonable expectation of privacy. The government's request is covered by existing law - namely, the *Fourth Amendment's* probable cause requirement, *Rule 41*, and ECPA - and the government makes no allegations of extraordinary circumstances that would justify deviation from that existing law. Indeed, the government does not suggest that the subject of the arrest warrant in this case has done or is likely to do anything to "frustrate the implementation" of that arrest warrant. Cf. *N.Y. Tel. Co., 434 U.S. at 174* ("The power conferred by the Act extends, under appropriate circumstances, to persons who . . . are in a position to frustrate the implementation of a court order or the proper administration of justice"). But, the government complains, the Court's denial of the warrant establishes a "head start" rule: "before the government

could obtain an order to locate the subject of an arrest warrant, the defendant would have to be given notice of the warrant and thus a head start in which he could begin avoiding arrest." (ECF No. 10, 7). That is not the case. Indictments are routinely sealed to allow apprehension using traditional investigative means before publication [*164] of the charges. Moreover, there are constitutional limitations on law enforcement actions which undoubtedly impede effectiveness. The Court acknowledges that a defendant has no "right" to turn himself in. [35] But that does not mean that the government has an unfettered right to pursue him.

35 The prosecutor has discretion to initiate prosecution either by summons or warrant, and is not required to demonstrate anything more in terms of danger or likelihood of flight to receive an arrest warrant, rather than a summons. *Fed. R. Crim. P. 4*.

Importantly, the government's request, if granted, would infringe on different rights than those implicated by an arrest warrant, as the government seeks to obtain ongoing precise location data over an extended period of time rather than a onetime search for the subject himself, at a specific place.

The government simply cannot use the All Writs Act to circumvent the requirements of the *Fourth Amendment* and other statutes that already occupy the space. The All Writs Act will allow the Court to take the necessary steps to effectuate its orders, but only where all other means have been exhausted. The government has not exhausted its remedies here and has demonstrated [*165] no exceptional circumstances that would justify an extraordinary writ.

Moreover, application of the All Writs Act to government requests for location data would have the ill-advised result of effectively exempting this and future similar requests from the congressionally-mandated reporting requirements that accompany orders and warrants established by the Rules and statutes discussed herein. An extensive congressional scheme provides courts with guidance as to the form and substance of the authorizations. See *18 U.S.C. ß 2518 (1)-(4)* (outlining authorization application requirements, probable cause standard, form of court order, and allowances for status updates applicable to orders authorizing or approving the interception of a wire, oral, or electronic communication under *18 USCS ßß 2510 et seq.*); *18 U.S.C. ß 2703(c)* (specifying types of authorizations (warrant, order, subpoena) required for obtaining information and requirements for each). By contrast, if a cell phone used for this purpose were classified as a tracking device, specified reporting requirements would automatically apply. See *Fed. R. Crim. P. 41(f)(2)*. This Rule outlines reporting requirements for use of tracking devices. [*166] Id. Moreover, this Rule requires that notice be provided to the tracked person after the end of the use of the device, id., but does provide for delayed notification, *id. at (f)(3)*. Delayed notification requires additional reporting of grants/extensions/denials of these warrants to the Administrative Office of the United States Courts. See *18 U.S.C. ß 3103a(d)*.

As Justice Powell noted in Pa. Bureau of Corr., "[a]lthough the Act empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate." *474 U.S. at 43*. Here, in the absence of extraordinary circumstances, where statutory law properly governs the government's request and unlike N.Y. Telephone Company, Congress most certainly has not endorsed acquisition of location data for this purpose, the Court will not allow the government to ignore the restrictions of the *Fourth Amendment* and circumvent the protections

established by statute by invoking the All Writs Act. Therefore, the government's application under the All Writs Act is unavailing.

III. CONCLUSION

As set forth above, the Court [*167] finds that real time, precise location data generated by a cell phone is entitled to a reasonable expectation of privacy and thus is subject to the *Fourth Amendment's* protections and the procedural requirements of *Rule 41*. This information is not exempted from *Rule 41*, as the Court further finds that location data is not an "electronic communication," cell phone providers are "electronic communications services" except to the extent a cell phone is used as a tracking device, and to the extent prospective location information is generated and/or requested a cell phone is classified as a tracking device.

This Court has articulated a procedure for requesting prospective, real time location information:

> When the government seeks to acquire and use real time cell site information to identify the location and movement of a phone and its possessor in real time, the court will issue a warrant upon a sworn affidavit demonstrating probable cause to believe the information will yield evidence of a crime. The court will not enter an order authorizing disclosure of real time cell site information under authority other than *Rule 41*, nor upon a showing of less than probable cause.

In re Application of the United States . . ., 402 F.Supp.2d at 605. [*168] [36] For the reasons articulated above, the Court finds that requests for GPS or any other precise location information generated by, for, or in relation to a cell phone are subject to the same standard. This standard is met if the affidavit provides that: a valid arrest warrant has issued for the user of the subject cell phone; the subject cell phone is in the possession of the subject of the arrest warrant; and the subject of the arrest warrant is a fugitive, that is, has demonstrated intent to flee to avoid prosecution.

> 36 The issue in this case was not use of location data to locate a defendant but the standard of proof required to acquire location data in a criminal investigation, but the procedure applies equally here.

Rule 41(b) provides that a tracking warrant may be used up to 45 days. *Fed. R. Crim. P. 41(b)*. That would appear to be unnecessarily long in most fugitive situations. The Court shall grant a tracking warrant until the subject of the arrest warrant has been located or a reasonable number of days under the circumstances, whichever is sooner. The duration of the tracking warrant must be tailored to the purpose of the warrant, here, the apprehension of the subject of the [*169] arrest warrant. *Arizona, 480 U.S. at 324-25* ("Taking action, unrelated to the objectives of the authorized intrusion, which exposed to view concealed portions of the apartment or its contents, did produce a new invasion of respondent's privacy unjustified by the exigent circumstance that validated the entry."); *Maryland, 480 U.S. at 86-87* ("[T]he purposes justifying a police search strictly limit the permissible extent of the search.); Cf. *Wilson, 526 U.S. at 612* ("[T]he *Fourth Amendment* does require that police actions in execution of a warrant be related to the objectives of the authorized intrusion."). Surveillance after the subject of the arrest warrant is located would have to be justified on another basis; otherwise, it would appear to be solely for impermissible, investigative purposes.

As requests for location information are governed by existing federal law, these requests do not present extraordinary situations that justify invocation of the All Writs Act or any other inherent power of this Court. All government requests are subject to the *Fourth Amendment*. Having found that the government's request for location data fails to establish probable cause and, specifically, a nexus [*170] between the information sought and the alleged crime, the government's applications are hereby DENIED. This denial does not frustrate or impede law enforcement's important efforts, but rather places them within the constitutional and statutory framework which balances citizens' rights of privacy against government's protection of society. It does place precise location information out of the government's casual reach. It requires that the government meet a certain threshold requirement - a showing that the information sought is evidence of a charge under *ß 1073* or evidence of another crime - prior to infringing upon a person's individual privacy rights. If you are not in a public place, there is a right to anonymity of your location. If you are in a private place, you have a right to anonymity of your movements in that place. Some courts would hold that if you are in a public place, you have the right to anonymity of your movement, especially if surveilled continuously for any significant period of time.

There is no precedent for what the government seeks: the right to obtain location data without any demonstration of the subject's knowledge of, and attempt to avoid, an arrest warrant. [*171] While courts routinely authorize location data where there is a demonstration under *Rule 41(c)(1)* that a defendant is fleeing to avoid prosecution and a few courts have authorized other types of surveillance in aid of an arrest warrant under All Writs Act where diligent law enforcement techniques have failed or been frustrated, no court under any rubric has approved a warrant or order for location data on the simple showing of an outstanding arrest warrant and the possession of a cell phone by the subject of the arrest warrant. See, e.g., *In the Matter of the Application . . ., 727 F.Supp. 2d 571, n.22 (W.D. Tex. Jul. 29, 2010)* (stating that, in a case in which the government seeks location data to track a person so that an arrest warrant may be executed, the warrant affidavit must demonstrate the existence of the arrest warrant and probable cause to believe that the phone is in the possession of the fugitive)(emphasis added); *In the Matter of Application for an Order . . ., 439 F.Supp. 2d 456* (denying government's application for an order authorizing access to prospective cell site information where the government failed to submit an affidavit attesting to the facts in the application, [*172] including the defendant's fugitive status).

The government's arguments, if credited, would allow law enforcement to obtain location data on any subject of an arrest warrant. This would be the result whether the defendant was charged with a misdemeanor or a felony, without any demonstration of any attempt on the part of the subject to avoid prosecution, so long as law enforcement had reason to believe that the source of the location data - here a cell phone - was in the possession of the subject.

Some might say that this is an appropriate use of a new technology in the service of more efficient and effective law enforcement. Others might say it is an unnecessary use of a new technology in a society already subjected to pervasive surveillance. The Court understands the tension. Regardless of individual views, the law does not currently sanction the requested acquisition of location data in these circumstances.

Date: 8/03/2011

/s/ Susan K. Gauvey

United States Magistrate Judge