Cell-Site Data Cases

DEA's capture of defendant's cell-site data did not violate the defendant's Fourth Amendment or Title III rights. Assuming without deciding that cell-site data fits within the definition of "electronic communication," the Court points out that suppression is not a permissible statutory remedy under Title III for the illegal interception of an electronic communication. 18 U.S.C. 2510(1)(c). (The Court finds that a strong argument exists that cell-site data is not a form of communication at all, in that it is not a message and it is not exchanged between individuals, but is just data sent from a cellular phone tower to the provider's computers.) Under the rationale of U.S. v. Knotts, 460 U.S. 276 (1983), the defendant has no legitimate expectation of privacy in the cell-site data because a person has no reasonable expectation of privacy regarding his travel on public thoroughfares, and the surveillance agents could have obtained the same information by following the defendant's car on the public highways. DEA simply used the cell-site data to "augment" sensory faculties, which is permissible under Knotts. Defendant's argument that DEA's use of the defendant's cell-site data effectively turned his cell phone into a tracking device within the meaning of 18 U.S.C. 3117, undermines the defendant's contention that suppression is appropriate under Title III. The definition of "electronic communication," 18 U.S.C. 2510(12)(C), excludes "any communication from a tracking device (as defined in section 3117 of this Title)" and thereby removes such tracking device communications from Title III coverage. Assuming, moreover, that the defendant is correct in his assertion that his phone was used as a tracking device, § 3117 does not provide a suppression remedy. See U.S. v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000), where the court observed that, in contrast to other statutes governing electronic surveillance, § 3117 "does not *prohibit* the use of a tracking device in the absence of conformity with the section.... Nor does it bar the use of evidence acquired without a section 3117 order." (Emphasis in original.) The Court finds Gbemisola to be persuasive and likewise concludes that § 3117 does not provide a basis for suppressing the cell-site data. Defendant attempted to distinguish his case from Smith v. Maryland, 442 U.S. 735 (1979) in that he did not voluntarily convey his cell-site data to anyone, and did not in fact use his cell phone. The agent dialed defendant's cell phone and the dialing caused the phone to send signals to the nearest cell tower. The Court, however, finds that the distinction between the cell-site data and the defendant's location is not legally significant under the particular facts of this case. The cell-site data is simply a proxy for the defendant's visually observable location as to which the defendant has no legitimate expectation of privacy. The Supreme Court's decision in Knotts is controlling. The DEA agents did not conduct a search within the meaning of the Fourth Amendment when they obtained the defendant's cell-site data. U.S. v. Forest, 355 F.3d 942 (6th Cir. 2004).

Magistrate judges in several federal districts have issued opinions rejecting the Government's "hybrid" theory that orders authorizing the prospective acquisition of cell site information can be obtained under the combined authority of the pen/trap statute and the provisions of 18 U.S.C. 2703. In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 10/14/05); In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294 (E.D.N.Y. 10/24/05); In the Matter of Applications of the United States of

America for Orders Authorizing the Disclosure of Cell Site Information, 2005 WL 3658531 (D. D.C. 10/26/05); In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [sealed] and [sealed] and the Production of Real Time Cell Site Information, 402 F. Supp. 2d 597 (D. Md. 11/29/05); In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D. D.C. 2005); In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134 (D. D.C. 2006); In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wis. 2006) (affirmed by district judge 10-6-06; see opinion note below); In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification Number (585) 111-1111 and the Disclosure of Subscriber and Activity Information Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); In the Matter of the Application of the United States of America for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed], 416 F. Supp. 2d 390 (D. Md. 2006); In re Application of the United States of America for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 2006 WL 468300 (S.D.N.Y. 2/28/06); In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information, 497 F. Supp. 2d 301 (D. P.R. 2007). The government maintains that: cell-site information is "dialing, routing, addressing, or signaling information" under the pen/trap statute; cell-site information is "a record or other information pertaining to a subscriber or customer" of an electronic communication service provider under ECPA; the government is not required to obtain a probable cause warrant (nor is it required to invoke the authority of the tracking device statute, 18 U.S.C. § 3117) to compel disclosure of cell-site information; and cell-phone users do not have a reasonable expectation of privacy in cell-site information.

On June 26, 2006, a district judge in the Northern District of Indiana denied the government's appeal of a magistrate judge's denial of two applications for cell site information: "The conclusion reached is the same as that of the Magistrate in his Order denying the applications, specifically: (1) the Government cannot rely on the Pen Register Statute to obtain cell site location information; and (2) converging the Pen Register Statute with the SCA in an attempt to circumvent the exception in the CALEA is contrary to Congress' intent to protect cell site location information from utilization as a tracking tool absent probable cause under the Fourth Amendment." In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services, 2006 WL 1876847 (N.D. Ind.) (7-5-06 amendment of 6-26-06 opinion).

On July 19, 2006, Southern District of Texas Magistrate Judge Smith granted, in part, the government's application for a pen/trap order, but denied the Government's request that the pen/trap include post-cut-through dialed digits. In recent years, pen/trap applications have

routinely included a request for inclusion of post-cut-through dialed digits. An explanatory footnote usually would be included in the application. MJ Smith maintains that the pen/trap statute prohibits the acquisition of any content. In addition, MJ Smith reiterates and expands on his 10-14-05 (396 F. Supp. 2d 747) legal analysis to once again reject the government's hybrid theory for the prospective acquisition of cell site data acquisition. In re U.S., 441 F. Supp. 2d 816 (S.D. Tex. 2006).

On July 24, 2006, District of Maryland MJ Bredar issued a letter opinion denying the government's pen/trap request for prospective cell-site information to capture a fugitive. MJ Bredar insisted that the government provide a sworn Rule 41 affidavit notwithstanding that the pen/trap application contained ample probable cause. The government replied that it considers this a test case for its 3123/2703 hybrid theory, and therefore the government would decline to provide the sworn affidavit.

> MJ Bredar:
>
> On July 20, the government submitted an application for, *inter alia*, a court order authorizing the use of a pen register to capture and report prospective cell site information for the purpose of tracking a fugitive. Upon reading the application, I found that it amply demonstrated probable cause, and I communicated this finding to the government informally. I also advised the government that I would immediately issue a warrant under Rule 41, Fed.R.Crim.P., if the government provided a sworn affidavit attesting to the facts in the application. This apparently being a fugitive investigation, the urgent nature of the request was not lost on me.
>
> The government responded that, although it could provide such an affidavit, it would not do so because it considered this a test case for its position that an order to obtain prospective cell site information can be entered upon less than probable cause pursuant to the combined authority of 18 U.S.C. § 3121 *et seq.* (the "Pen/Trap Statute") and 18 U.S.C. § 2701 *et seq.* (the "Stored Communications Act") provided the government offers "specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and material to an ongoing criminal investigation." [FN1] 18 U.S.C. § 2703(d).

In Matter of Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the Number [sealed], 439 F. Supp. 2d 456 (D. Md. 2006).

On October 6, 2006, a district judge in the Eastern District of Wisconsin affirmed a magistrate judge's rejection of the government's application for the acquisition of prospective cell-site data. "I find that cell site information should be obtained under Fed. R. Crim. P. 41 and § 3117(b), or § 2518, rather than the Pen/Trap statute coupled with the SCA. Additionally, I find unpersuasive the government's contention that the SCA, coupled with the Pen/Trap statute, provides adequate supplemental authority." In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 2006 WL 2871743 (E.D.

Wis.).

On December 20, 2005, a S.D.N.Y. magistrate judge issued an opinion supporting the Government's combined 3123/2703 approach to obtaining orders for prospective acquisition of cell site information. Such an order is limited to information identifying the cell tower and the affected portion of the antenna; tower information tied to a particular telephone call made or received by the user; and information that is transmitted from the provider to the Government. If the Government seeks to obtain other information, the court requests additional briefing on why such information is permissible under the relevant authorities. In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 12/20/05). The following opinions were issued by magistrate judges in agreement with the 12/20/05 SDNY MJ opinion: In the Matter of the Application of the United States for an order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 411 F. Supp. 2d 678 (W.D. La. 1/26/06); In re Application for an Order Authorizing the Installation and Use of a Pen Register Device, Trap and Trace Device, Dialed Number Interceptor, Number Search Device, and Caller Identification Service, and the Disclosure of Billing, Subscriber, and Air Time Information, No. S-06-SW-0041 (E.D. Cal. 3/15/06).

On April 11, 2006, a district judge in the Southern District of Texas, favorably citing the 12/20/05 SDNY, 1/26/06 WDLa, and 3/15/06 EDCal MJ opinions, issued a pen/trap/2703(d) order authorizing the prospective acquisition of cell site information tied only to telephone calls actually made or received by the telephone user. The judge noted that the government is not seeking to activate the telephone's GPS functionality; is not seeking to obtain information from multiple cell towers simultaneously to "triangulate" precise locations; and is not seeking to place calls to the target telephone repeatedly or otherwise to track on a continuous basis the location of the telephone when no call is being placed or received. In the Matter of the Application of the United States for an order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, 433 F. Supp. 2d 804 (S.D. Tex. 4/11/06).

On October 23, 2006, Judge Kaplan of the S.D.N.Y. issued an opinion accepting "the government's argument that the Pen Register Statute and the Stored Communications Act, combined pursuant to CALEA, permit a court to authorize the disclosure of prospective cell site information, at least where, as here, the government does not seek triangulation information or location information other than that transmitted at the beginning and end of particular calls." The court noted, however, that there is no reason to believe that the government's combined application approach would not authorize disclosure of cell site information from multiple antenna towers simultaneously. In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006).

On February 1, 2007, a magistrate judge in the Eastern District of California held that FRCP 41, as amended December 1, 2006, does not require a warrant based on probable cause for cell site information, at least where the subject of the cell site tracking is outside of a home or other

expected place of privacy. The Supreme Court has acknowledged that the standard for installation of a tracking device is unresolved. The amended Rule 41 does not resolve this issue. Legislative history indicates that the 18 U.S.C. 3117(b) definition of "tracking device," passed in 1986, is confined to the transponder type devices placed upon the object or person to be tracked. Nothing in the amendment to Rule 41 was meant to change the prior law concerning the necessity for the warrant in the first instance. The magistrate judge, in a previous order, had found that cell site location was subscriber information accessible to law enforcement under the authority of the pen/trap statute, Stored Communications Act and CALEA. In re Application for an Order Authorizing the Extension and Use of a Pen Register Device etc., 2007 WL 397129 (E.D. Cal.).

A magistrate judge in the S.D.W.Va. issued a pen/trap order that includes cell site location information solely pursuant to the pen/trap statute. Because the fugitive whose capture was being sought was the user of the target phone, but not the subscriber, the MJ found it unnecessary to reach the 3123/2703 convergence issue involving prospective cell site information acquisition raised by the government in a letter brief filed with its application. The MJ opined: "The user of a cell phone who is not the subscriber has no protection pursuant to 47 U.S.C. § 1002(a)(1). In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register with Caller Identification Device and Cell Site Location Authority on a Certain Cellular Telephone, 415 F. Supp. 2d 663 (S.D.W.Va. 2006).

On July 6, 2007, Southern District of Texas Magistrate Judge Smith, after a DAAG authorized an emergency pen/trap under the provisions of 18 U.S.C. 3125(a) for the use of a "mobile phone tracking device," denied the government's application for a 2703 order authorizing disclosure of location-based communications services, including "Enhanced 911" services relating to a pre-paid cellular telephone. The government made no request for pen/trap authority under 3123. The judge noted that he had no authority under 2703 to compel the service provider to create E-911 records, which the government candidly admitted the phone companies do not typically create or maintain. Judge Smith also noted, as he has previously held, that a mobile phone tracking device is not a pen/trap device; that amended Rule 41 expressly authorizes the use of tracking devices as that term is defined under 18 U.S.C. 3117(b); and that Rule 41 is the appropriate vehicle for tracking a cell phone's E-911 features. Ultimately, Judge Smith denied the application as moot because the phone company was unable to provide the information and was not currently providing it. In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Location Based Services, 2007 WL 2086663 (S.D. Tex.).

On September 17, 2007, in the District of Massachusetts, District Judge Stearns, on the government's appeal of Magistrate Judge Alexander's refusal (509 F. Supp. 2d 64) to grant the government's request for a 2703(d) order to obtain historical cell site information, reversed the Magistrate Judge's decision and granted the government's application. In re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76 (D. Mass. 2007).

On October 17, 2007, Judge Lee H. Rosenthal, Southern District of Texas, issued an opinion (includes overview of pen/trap cell-site jurisprudence) in response to the Government's request for a more expansive order after Magistrate Judge Smith granted the Government's request for

pen/trap authority but denied access to cell-site information and post-cut-through dialed digits. The judge opined as follows:

As to cell site data:

> The Government has made the necessary showing under the statutes and has sought limited information within the statutes' authorization. The Government is entitled to obtain the cell-site information it seeks, limited to a single antenna tower at one time for: (1) the origination of a call from the Target Device(s) or the answer of a call to the Target Device(s); (2) the termination of the call; and (3) if reasonably available, during the progress of the call. The cell-site data may not be sent directly to the Government, but must be recorded and stored by the cell phone provider first. The Government may not use or activate any GPS tracking on the Target Devices and may not place repeated calls to the cell phones in an effort to continuously track the location of the subscriber(s) or customer(s) using the Target Devices. The Government may not obtain prospective cell-site data when the phone is idle, that is, when a call is not being placed or received on the Target Devices.

As to PCTDD:

> The Pen Register Statute expressly prohibits the collection of content. The Government may not get around this prohibition simply by acknowledging that there is no reasonably available technology to prevent the collection of content. Nor can the Government get around the prohibition by asserting that it will not use any content it collects for investigative purposes. Unlike the Wiretap Act, the Pen Register Statute does not permit the Government simply to minimize the effects of its collection of unauthorized content, but instead prohibits the collection of content in the first place. The Pen Register Statute does not authorize the Government to collect post-cut-
> through dialed digits when there is no reasonably available means to prevent the collection of content. If the Government has no means to exclude collecting content when collecting post-cut-through dialed digits, the Government may not obtain such information under the Pen Register Statute. The Government's requests in its pen register applications for post-cut-through dialed digits are denied.

In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, 2007 WL 3036849 (S.D. Tex.).

On November 6, 2007, Magistrate Judge Alexander, in the District of Massachusetts, denied the Government's application for prospective cell site information because it was not based on probable cause. In re Applications of the United States of America for an Order Authorizing Continued Use of a Pen Register and Trap and Trace with Caller Identification Device and Cell Site Location Authority on Telephone Number (XXX) XXX-XXXX and Any Subsequently Assigned Telephone Number, 530 F. Supp. 2d 367 (D. Mass. 2007).

On November 7, 2007, a magistrate judge in the S.D. of Texas denied without prejudice the Government's application under 3122 and 2703 to obtain real time cell-site data and "Enhanced 911" information to identify the exact location of a cell phone. The Government failed to provide sufficient specifics and details to establish the requisite probable cause. In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and

Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services, 2007 WL 3355602 (S.D. Tex.).

On December 27, 2007, a magistrate judge in the Southern District of Texas denied the Government's 3122/2703 application for real-time cell site and "Enhanced 911" data on a cell phone because the application failed to establish probable cause as required by Rule 41 for "tracking device" warrants. The information attempting to link the subject with criminal activity was conclusory and unsubstantiated, and the subject was not linked to the target device. In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Installation and Use of a Mobile Tracking Device, 2007 WL 4591731 (S.D. Tex. 2007).

On February 19, 2008, five magistrate judges in the Western District of Pennsylvania jointly denied the Government's 2703(d) application for historic cell site location information (CSLI):

> Because this Court concludes that the Government does not have a statutory entitlement to an electronic communication service provider's covert disclosure of cell-phone-derived movement/location information, the Government's application(s) for such information, absent a showing of probable cause under Fed.R.Crm.P. 41, must be denied.

In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585 (W.D. Pa. 2008) (affirmed on appeal to district judge at 2008 WL 4191511, September 10, 2008).

On April 21, 2008, a magistrate judge in the Northern District of Georgia recommended that defendants' motion to suppress historical cell site information, obtained by the Government pursuant to a 2703(d) order, be denied. The court concluded that the defendants did not suffer any Fourth Amendment violation. U.S. v. Suarez-Blanca, 2008 WL 4200156 (N.D. Ga.) (unpublished).

On May 30, 2008, MJ Smith, S.D. Tex., issued a memorandum and order addressing "a recurring issue of electronic surveillance law not previously decided in a published case:" whether the electronic surveillance court orders [pen/trap, 2703(d), tracking device warrants issued by magistrate judges in the S.D. Texas] may properly be kept secret, by sealing and non-disclosure provisions, for an indefinite period beyond the underlying criminal investigation." MJ Smith concludes that setting a fixed expiration date on sealing and non-disclosure of such orders is not merely better practice, but required by the First Amendment prohibition against prior restraint of speech and the common law right of public access to judicial records. A survey of electronic surveillance orders issued by magistrate judges in the S. D. Tex. for the period 1995-2007 showed that 91.6% of the 4234 electronic surveillance orders issued during this period remain completely sealed. Almost all provide that they are sealed "until further order of the court." MJ Smith chooses a default 180 day period for sealing and non-disclosure, after which the orders will be unsealed and disclosable unless the Government moves to extend the ban for another 180 days based on (a) a certification that the investigation is still active or (b) a showing of

exceptional circumstances. Additional extensions will require correspondingly greater specificity in the certification. The Government will given a 30 day advance notice before the gag orders are lifted and unsealed. In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876 (S.D. Tex. 2008).

On June 9, 2008, MJ Orenstein, EDNY, issued a memorandum and order explaining why he issued orders, based upon probable cause, for the real time acquisition of latitude and longitude data associated with specified telephones, but removed the Government's citation to authority under Rule 57(b) and the All Writs Act (except as it applies to the court's direction to the service provider to maintain the secrecy of the instant matter), and issued the order "pursuant to Fed. R. Crim. P. 41 and 18 U.S.C. § 3117, denied the Government's request to delay notification under 3103a until underlying criminal investigation eavesdropping materials are unsealed, but no later than 365 days from date of order, and instead authorized an initial 30 day delay pursuant to Rule 41(f)(2)-(3) and 18 U.S.C. 3103a, with the possibility of a 90 day extension upon an updated showing of the need for further delay. MJ Orenstein opined that the Government need only show Fourth Amendment probable cause because no statute creates a heightened standard and the recent amendment to Rule 41 suggests there is none. The "super-warrant" requirements for wiretaps are a creature of statute. In the Matter of an Application of the United States of America for an Order Authorizing the Disclosure of Latitude and Longitude Data Relating to a Specified Wireless Telephone, 2008 U.S. Dist. LEXIS 45311 (E.D.N.Y.).

On November 26, 2008, E.D.N.Y, Judge Garaufis joined the minority of courts concluding that the Government may obtain prospective cell-site information pursuant to its so-called "hybrid theory" without a showing of probable cause. The order authorizes service providers to provide the Government with information which identifies the cell tower and face transmitting calls to or from the target telephones at the beginning and end of calls. The order does not permit the Government to receive triangulation information or location information other than that transmitted at the beginning and end of particular calls. In the Matter of an Application of the United States of America for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202 (E.D.N.Y. 2008).

On December 16, 2008, EDNY MJ Orenstein acknowledged the 11/26/08 opinion of district judge Garaufis, but asserts his independence from precedential control by a single district judge. Regarding a routine application for pen/trap coverage of cell phone, MJ Orenstein ordered that unless PCTDD are routinely recorded by the service provider in the absence of a court order and PCTDD will be removed by the service provider before the pen/trap data is sent to the government, the pen/trap application is denied. MJ Orenstein does not accept the government's proposal to delete PCTDD after receipt from the service provider. Orenstein finds no legal authority for such post-recording excision by the government, nor does Orenstein find any legal authority that allows one government agent, but not others, to access recorded PCTDD content. In the Matter of an Application of the United States of America for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device on Wireless Telephone Bearing Telephone Number [Redacted], Subscribed To [Redacted], Serviced by [Redacted], 2008 WL 5255815 (E.D.N.Y.).

On January 13, 2009, SDNY Judge McMahon, affirmed Magistrate Judge Ellis's refusal to issue

an order authorizing disclosure of prospective CSLI:

> Even if I am wrong about the foregoing [cell phone is a tracking device and provider of CSLI does not fall within the statutory definition of "electronic communication service"], and a cell phone provider is in fact an "electronic communications service" within the meaning of the SCA, I also note that 18 U.S.C. § 2703(c) only authorizes the Government to require a "provider of electronic communication service" to disclose "a record or other information" *about "a subscriber ... or customer ....*" of such a service. (Emphasis added). I question whether CSLI qualifies as "a record or other information" about a *subscriber* or *customer*. As a technical matter, CSLI does not provide information about a particular person or entity (and a subscriber or customer is necessarily a person or entity), Rather, it constitutes "a record or other information" about *the cell phone*--specifically, about the location of the cell phone at a specific moment in time. It does not and cannot disclose whether the person whose movements are being tracked by the CSLI is the cell phone provider's "subscriber" or "customer."

Judge McMahon observes that the Government may obtain the CSLI with a Rule 41 warrant, and suggests that Congress make appropriate corrections to the statute to reflect advances in cell phone technology. In the Matter of an Application of the United States of America for an Order Authorizing the Use of a Pen Register With Caller Identification Device Cell Site Location Authority on a Cellular Telephone, 2009 WL 159187 (S.D.N.Y.).

On February 12, 2009, EDNY Magistrate Judge Pollak granted two and denied one government request for prospective cell site data sought in three hybrid 3123/2703 applications. The judge concluded that since probable cause sufficient to satisfy Rule 41 is required to obtain an order authorizing the use of a more traditional tracking device such as a GPS device, and given the fact that the government conceded in one of its applications that technology is now available that allows the government, through the instantaneous acquisition of cell-site information, to transform the cell phone into a tracking device superior to the GPS device then in use by the government (time delay made exact location determination impossible), it would be incongruous to require less than probable cause for disclosure of prospective cell-site information that actually provides a more precise ability to track and locate an individual. Two of the applications contained sufficient probable cause, but the third application did not contain probable cause and therefore that portion of the application seeking prospective cell-site information was denied. The judge recognized that extensive analysis of the interaction between the SCA and the pen/trap statute has already been conducted, but felt compelled to emphasize that the SCA and CALEA intended to treat tracking information differently, and that if Congress intended the convergence of the pen/trap statute and the SCA statutes, it generally does so explicitly. The judge also emphasized that the SCA appears designed to compel disclosure of information that is historical, not prospective–i.e., information stored at the time a court order is issued. "Thus it is unclear to this Court that where the conceded purpose of the application is to obtain prospective information made available instantaneously so as to enable the government to track a person in real-time, this information constitutes a "stored communication." In the Matter of the Application of the United States of America for an Order Authorizing (1) the Use of a Pen Register and Trap and Trace Device With Prospective Cell-Site Information and (2) the Release of Historical Cell-Site and Subscriber Information, 2009 WL 1530195 (E.D.N.Y.). [Reversed on 2/26/09 by Judge Garaufis, Misc. 09-104]

On March 19, 2009, Judge Pauley of the S.D.N.Y. supported the Government's use of a hybrid 3123/2703(d) order to track a cell phone being used by the driver of a tractor-trailer as it traveled across the United States to the New York metropolitan area with 230 kilograms of cocaine

concealed in the trailer of the truck. "Navas did not have a legitimate expectation of privacy in the cell phone. First, the cell phone was only utilized on public thoroughfares en route from California to New York; there is no indication that law enforcement ever surveilled Navas, or any of the Defendants, in a private residence. Second, Navas was not a subscriber to the phone. Finally, if Navas intended to keep the cell phone's location private, he simply could have turned it off. . . Accordingly, Navas did not have a reasonable expectation of privacy in the cell phone's transmissions and his motion to suppress based on information obtained under the Cell Site Order is denied.". Judge Pauley favorably cited fellow Judge Kaplan's October 23, 2006 (see above) opinion endorsing the Government's use of the 3123/2703(d) hybrid order to prospectively acquire cell site data. U.S. v. Navas, 640 F. Supp. 2d 256 (S.D.N.Y. 2009). [Government appealed district court's suppression of warrantless seizure of narcotics from unhitched trailer. Second Circuit reversed and held that it is the "inherent mobility" of an unhitched trailer, not the probability or potentiality of movement, that triggers the automobile exception to the Fourth Amendment's warrant requirement. U.S. v. Navas, 597 F.3d 492 (2nd Cir. 2010)]

On May 21, 2009, Northern District of Illinois Chief Judge Holderman denied the Government's request for a 3123/2703(d) hybrid order seeking, among other things, the prospective disclosure of cell site information on a real-time basis. The Court held that the law requires the government to support an application for real-time cell site information with probable cause. In the Matter of the Application of the United States of America for an Order Relating to Target Telephone 2, 733 F. Supp. 2d 939 (N.D. Ill. 2009).

On July 29, 2010, a magistrate judge in the Western District of Texas opined that he will insist on strict adherence to Rule 41 procedures for tracking device warrants on all requests for cell site location information, including requests for historical data.

> In sum, there are difficult questions presented by the probable cause determination on CSLI applications, and it is not obvious what the answers to those questions are (at least it is not obvious to me what the answers are). Accordingly, until there is more guidance from Congress and the courts on these issues, I will take a cautious approach toward CSLI requests. First, I will insist on strict adherence to the requirements of Rule 41 on all requests for CSLI, including requests for historical data. The warrants will be granted only on a showing of probable cause, may only last 45 days (in the case of prospective warrants), and notice on the person tracked is required (although it may be delayed). The warrants must be returned to the magistrate judge identified on the warrant. I will further require that warrants for CSLI be "stand alone" documents, and not be included as part of an application for a pen register, trap and trace, or subscriber records. With regard to probable cause, I will not take as narrow an approach as Judge Facciola's and insist that the CSLI must itself qualify as "evidence of a crime." But the warrant affidavit must demonstrate that there is probable cause to believe that tracking the phone will *lead* to evidence of a crime.

In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services, 727 F. Supp. 2d 571 (W.D. Tex.2010).

On August 27, 2010, EDNY Magistrate Judge Orenstein opined that he would refuse to issue an order for two months of historical cell site information in response to the Government's

application pursuant to the authority in 18 U.S.C. 2703(d). The Government refused to acquiesce in the judge's demand that it submit an affidavit or affirmation under FRCP 41 for a warrant. The judge discusses recent jurisprudential developments in this area, especially the opinion in U.S. v. Maynard, 2010 WL 2010 WL 3063788 (D.C. Cir.). The Government's reliance on 2703(d) is deemed insufficient to overcome the simple fact that 26 years of legislation does not explicitly address Fourth Amendment privacy issues raised by law enforcement's warrantless use of today's powerfully efficient and intrusive surveillance technology. In the Matter of the Application of the United States of America for an Order Authorizing the Release of Historical Cell-site Information, 736 F. Supp. 2d 578 (E.D.N.Y. 2010).

On September 7, 2010, the Third Circuit held "CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination. Instead, the standard is governed by the text of § 2703(d). . .Because the statute as presently written gives the MJ the option to require a warrant showing probable cause, we are unwilling to remove that option although it is an option to be used sparingly because Congress also included the option of a § 2703(d) order. However, should the MJ conclude that a warrant is required rather than a § 2703(d) order, on remand it is imperative that the MJ make fact findings and give a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users." In the Matter of Application of the United Sattes of America for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government, 620 F.3d 304 (3d Cir. 2010). See commentary in DOJ and EDPa memoranda.

Agents investigating a narcotics trafficker made repeated "emergency" requests in December 2008 and January 2009 to the target's cellular carrier for real-time "cell site information" concerning his phone, following up each request with an administrative subpoena. This information – which revealed the target's travels from one city to another, and which enabled agents to take up visual surveillance – was subsequently mentioned in the "necessity" section (as an alternative investigative technique used previously) of the affidavit supporting a Title III application directed at the target's phone. After indictment, the defendant moved to suppress the fruits of the wiretap, including all derivative evidence. The district court denied the motion on several grounds. First, the court found that the information would have inevitably been obtained via the subpoenas in any event. In addition, the court held that the information "simply allowed the police to confirm the defendant's general location ... as he moved in plain view on public highways" (citing *Knotts*). Finally, the court held – without citing Franks v. Delaware, but in apparent reliance on its core reasoning – that "even if the tracking is excised from the affidavit for warrant, it would not have affected the existence of probable cause." U.S. v. Redd, 2010 WL 3892231 (D. Kan.).

In the course of investigating a murder, California police officers obtained two search warrants seeking (among other records) historical cell-site location information (CSLI) for 9 cell phones. After indictment on federal charges, a defendant moved to suppress the CSLI. The district court denied the motion on several grounds. First, the defendant failed to assert any proprietary interest in several of the phones. Second, the court held that there could be no reasonable expectation of privacy in the CSLI, comparing it to the non-content telephone toll records at issue in *Smith v. Maryland*. Third, the court analogized the CSLI to information

obtained from a GPS tracking device, invoking the Ninth Circuit's recent decision in *United States v. Pineda-Moreno*. Noting the Ninth Circuit's approval of the warrantless use of the tracking device in that case -- and further noting that "[t]he privacy interests implicated here pale in comparison to those implicated in *Pineda-Moreno*" because CSLI is not as accurate as GPS data – the court held that the information about the defendant's location "could have been obtained through physical observation." On this last point, the court explicitly found that the CSLI was not capable of revealing the defendant's activities inside a residence or other protected private space. U.S. v. Velasquez, 2010 WL 4286276 (N.D. Cal. Oct. 22, 2010).

In response to several applications by the government to obtain historical cell-site location information under 18 U.S.C. § 2703(d), a magistrate judge Smith held that such information is protected by the Fourth Amendment and unavailable except pursuant to a warrant based on probable cause. The magistrate asserted (erroneously) that cell-site information is equivalent to the increasingly precise data produced by "network-based" location methods (also known as "trilateration" or "triangulation"). Proceeding from this incorrect factual finding, the court held that government access to historical CSLI violates the Fourth Amendment in the same manner as the tracking device at issue in *United States v. Karo*. Further, the magistrate held that the government's request for 60 days' worth of historical CSLI triggered the "prolonged surveillance" threshold of the D.C. Circuit's Fourth Amendment "mosaic theory," as articulated in the latter court's recent *Maynard* decision. Finally, MJ Smith held that users do not voluntarily convey CSLI to their wireless carriers, and that the rationale of *Smith v. Maryland* is therefore inapplicable. In re Application of the United States of America for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010).

MJ Orenstein continues to hold (notwithstanding reversal by a district judge in a similar decision several months ago) that the Fourth Amendment requires a probable cause Rule 41warrant to access historical CSI. The judge favorably cites the recent opinions in Warshak (6th Cir.), Maynard (Jones) (D.C. Cir.), CSI: Pittsburgh (3d Cir.), and CSI: Houston (MJ Smith SDTex.). In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 2010 WL 5437209 (E.D.N.Y. December 23, 2010).

On February 16, 2011, EDNY MJ Orenstein granted a 2703(d) order on two phones for historical cell-site information pertaining to several brief periods. MJ Orenstein explained why he is not applying the Maynard mosaic theory, or opting under the Third Circuit opinion to require a probable cause showing in this instance. In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 2011 WL 679925 (E.D.N.Y.).

On April 26, 2011, a SDFL magistrate judge granted defendant's request to unseal the 2703(d) application and order by which the government obtained historical cell phone data. The defendant intends to challenge the legality of compelled disclosure of historical cellular data that occurs on less than a showing of probable cause. U.S. v. Johnson, 2011 WL 1584320 (S.D. Fla.).

On August 3, 2011, a magistrate judge issued an opinion explaining why she declined to issue a warrant for cell phone location information merely to locate the subject of an arrest warrant who was not shown to be a fugitive or otherwise engaged in criminal activity. 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, 2011 WL 3423370 (D. Md.).

On August 22, 2011, Judge Garaufis, Eastern District of New York, ruled that the Government's request for at least 113 days of cumulative cell-site-location records for an individual's cell phone constitutes a search under the Fourth Amendment, and consequently, such information may not be obtained without a warrant and the requisite showing of probable cause pursuant to 18 U.S.C. 2703(c)(1)(a) and Federal Rule of Criminal Procedure 41.

> Like in Kyllo, the court here confronts the question of what "limits there are upon this power of technology to shrink the realm of guaranteed privacy." *Id. at 33*. The advent of technology collecting cell-site-location records has made continuous surveillance of a vast portion of the American populace possible: a level of Governmental intrusion previously inconceivable. It is natural for Fourth Amendment doctrine to evolve to meet these changes. . .The cell phone has replaced the public telephone to near extinction; yet, to date Fourth Amendment doctrine has not developed to embrace the vital role the cell phone has come to play in private communication and the new Fourth Amendment challenges in creates. The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by "choosing" to carry a cell phone must be rejected. In light of drastic developments in technology, the Fourth Amendment doctrine must evolve to preserve cell-phone user's reasonable expectation of privacy in cumulative cell-site-location records. . .While the government's monitoring of our thoughts may be the archetypical Orwellian intrusion, the government's surveillance of our movements over a considerable time period through new technologies, such as the collection of cell-site-location records, without the protections of the Fourth Amendment, puts our country far closer to Oceania than our Constitution permits. It is time that the courts begin to address whether revolutionary changes in technology require changes to existing Fourth Amendment doctrine. Here, the court concludes only that existing Fourth Amendment doctrine must be interpreted so as to afford constitutional protection to the cumulative cell-site-location records requested here.

In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 2011 WL 3678934 (E.D.N.Y.).