UNCLASSIFIED
NON-RECORD

[redacted]

Equipment support: They need to have some [redacted]

Operational support: They will need some support in the [redacted] and ensuring the equipment is running properly, in each location. b3 b6 b7C b7E

[redacted]

P.S. If we support this, we'll need to use [redacted]

[redacted]

From: [redacted]
Sent: Monday, November 29, 2010 3:18 PM
To: [redacted]
Subject: FW: Equipment for [redacted] b6 b7C

UNCLASSIFIED
NON-RECORD

What does he need??

SSA [redacted]
Unit Chief
Tracking Technology Unit
Operational Technology Division
[redacted]

From: [redacted]
Sent: Monday, November 29, 2010 3:13 PM
To: [redacted]
Subject: Equipment for [redacted] b6 b7C b7E

UC [redacted]

This is SSA [redacted] from the [redacted] unit. Recently I visited [redacted] down in your unit and we discussed various technologies [redacted] that were of use to the field. I followed up with an EC that I believe you guys have seen. Im just wondering what steps I need to take now in order to get the equipment out the field etc. I spoke with [redacted] earlier today and he said to contact you. Whatever you guys need from me please just let me know and ill get on it. I know the field is really looking forward to getting/using the equipment! Thanks a lot [redacted]

SSA [redacted]
[redacted]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~SECRET~~

DATE: 11-06-2012
CLASSIFIED BY 65179 DMH/rs
REASON: 1.4 (c, g)
DECLASSIFY ON: 11-06-2037

[redacted]

From: [redacted] b6 b7C
Sent: Tuesday, April 21, 2009 11:44 AM
To: [redacted]
Cc:
Subject: RE: [redacted]

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

SECRET//NOFORN
RECORD 268-HQ-1068430

b1 b3 b5 b7E

[redacted]

(S)

[redacted]

b6 b7C

-----Original Message-----
From: [redacted]
Sent: Tuesday, April 21, 2009 10:54 AM
To: [redacted]

~~SECRET~~

CELL/OTD 008487

~~SECRET~~

Cc:
Subject: RE:

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

b6
b7C

I will have my Engineer answer..

Can you provide answers..

SSA
Unit Chief
Tracking Technology Unit
Operational Technology Division

-----Original Message-----
From:
Sent: Tuesday, April 21, 2009 10:40 AM
To:
Subject: RE:

b1
b3
b5
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

(S)

Office
Cell:
BB:

b6
b7C

-----Original Message-----
From:
Sent: Tuesday, April 21, 2009 6:21 AM
To:
Cc: DICLEMENTE, ANTHONY P. (OTD) (FBI);
Subject: RE

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

I will forward to SC Diclementi for info..

I will stand down on requesting support on a 60 day TDY assignment..

P.S. I received the two cellular phones yesterday

~~SECRET~~

CELL/OTD 008488

~~SECRET~~

[redacted] FYI. Thought the [redacted] support was of interest!!!

SSA [redacted]
Unit Chief
Tracking Technology Unit
Operational Technology Division
[redacted]

b6
b7C

-----Original Message-----
From: [redacted]
Sent: Monday, April 20, 2009 6:52 PM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

b3
b5
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted]

[redacted]

UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

DERIVED FROM: Multiple Sources
DECLASSIFY ON: 20340421
SECRET//NOFORN

~~SECRET~~

CELL/OTD 008489

DATE: 11-07-2012
CLASSIFIED BY 65179 DMH/rs
REASON: 1.4 (c, g)
DECLASSIFY ON: 11-07-2037

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

[redacted]

From: [redacted] b3 b6 b7C b7E
Sent: Monday, July 13, 2009 4:27 PM
To: [redacted]
Subject: [redacted]

~~SECRET~~//NOFORN
RECORD 268-HQ-1068430 b1 b3 b5 b7E

[redacted]

(S)

(U) (~~S~~/NF) To implement this capability [redacted] b3 b6 b7C b7E

(S)

(U) (~~S~~/NF) On another note:

(U) (~~S~~/NF) To further support this event, I would like to request that we receive a [redacted] capability also developed by [redacted] which once we do all the work required mentioned above. [redacted] The [redacted] I think you'll get some kickback on [redacted] with them [redacted] although I would like to really give it a try. b3 b6 b7C b7E

[redacted]
cell: [redacted]

DERIVED FROM: Multiple Sources
DECLASSIFY ON: 20340713
~~SECRET~~//NOFORN

[redacted]

From: [redacted] b6 b7C
Sent: Thursday, October 12, 2006 1:57 PM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted] Trip Report to [redacted]

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

[redacted]

[redacted] b3 b5 b6 b7C b7E

[redacted]

[redacted]

[redacted]

[redacted]

Thanks,

b3
b5
b6
b7C
b7E

[redacted]
[redacted] - Nextel
[redacted] - Desk

-----Original Message-----
From: [redacted]
Sent: Tuesday, October 10, 2006 3:45 PM
To: [redacted]
Cc:
Subject: [redacted] Trip Report to [redacted]

b6
b7C

SENSITIVE BUT UNCLASSIFIED
NON-RECORD

The intent of this email is to provide a brief sypnosis of the events found, verified, and validated and to solicit feedback if the reported items are incomplete or inaccurate. A comprehensive white paper shall be produced, made available on the [redacted] website, and be announced to all of the [redacted] An EC shall also be forthcoming.

[redacted]

[redacted]

b3
b5
b7E

1) [redacted]

2) [redacted]

3) [redacted]

4) [redacted]

[redacted]

A [redacted] shall be presented in the white paper.

[redacted]

b3
b5
b6
b7C
b7E

SENSITIVE BUT UNCLASSIFIED

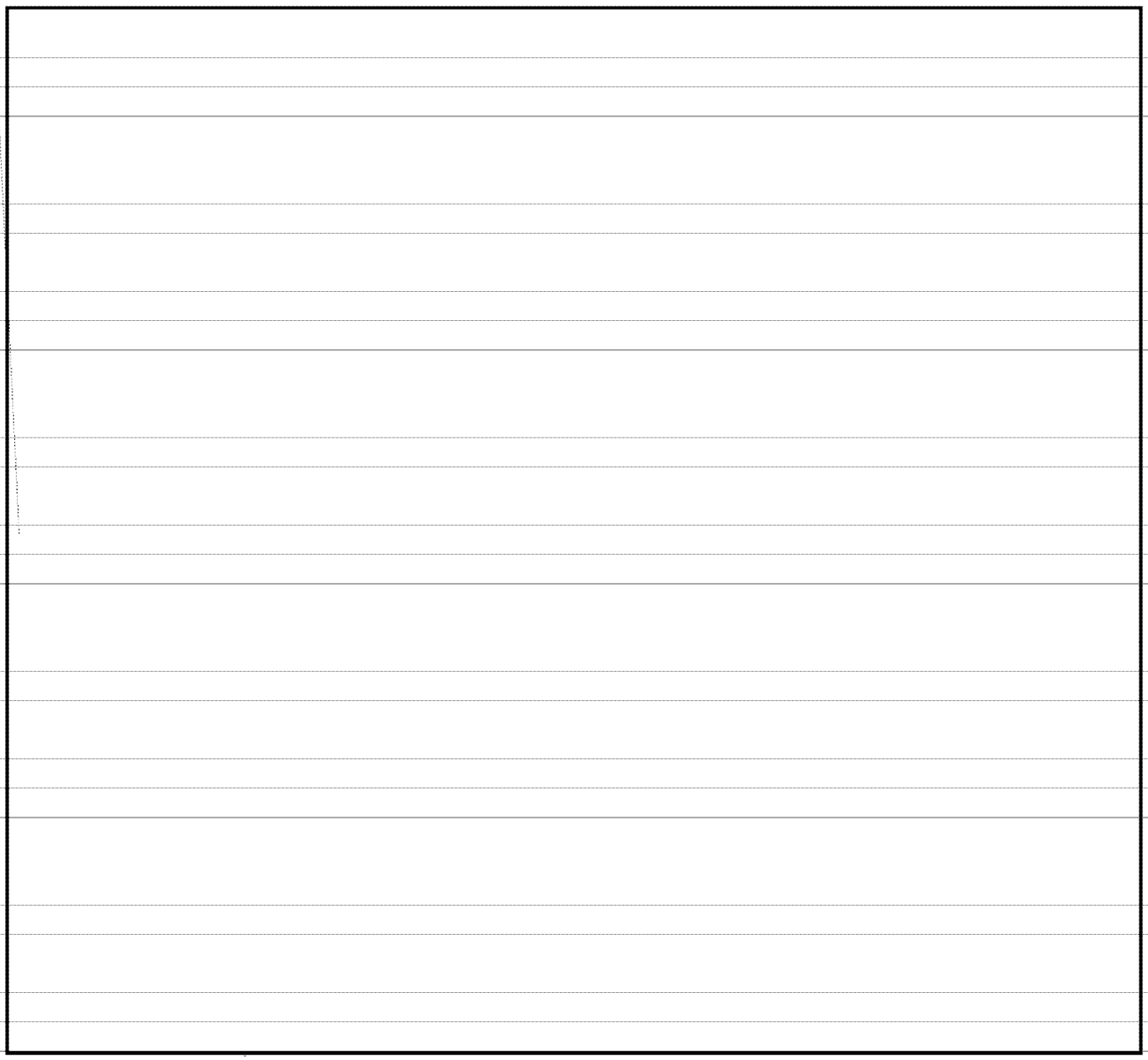
~~SECRET~~

DATE: 11-08-2012
CLASSIFIED BY 65179 DMH/rs
REASON: 1.4 (c, g)
DECLASSIFY ON: 11-08-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b3
b5
b7E

(S)



~~SECRET~~

[redacted]

From: [redacted]
Sent: Tuesday, November 04, 2008 6:27 PM
To: [redacted]
Subject: FW: OGC Guidance Concerning Requests for [redacted]

b3
b6
b7C
b7E

UNCLASSIFIED
NON-RECORD

[redacted]

Here is an OGC position on [redacted]

[redacted]
Assistant General Counsel
Science and Technology Law Unit
Office of the General Counsel
Federal Bureau of Investigation
(Office) [redacted]
(Cell) [redacted]
(Secure) [redacted]
(Fax) [redacted]

b3
b5
b6
b7C
b7E

From: [redacted]
Sent: Monday, November 03, 2008 3:03 PM
To: FBI_ALL_CDCs
Cc: [redacted]
Subject: OGC Guidance Concerning Requests for [redacted]

UNCLASSIFIED
NON-RECORD

This e-mail is being sent to all CDCs and ADCs,

A recent decision in the District Court for W.D. Pa. regarding the legal authority required to obtain historical cellular telephone location information has received widespread press coverage. Several CDC's have contacted us with questions. Because of the possibility that magistrate judges in your divisions may rely on this opinion, OGC provides the following guidance. b5

[redacted]

b5

[redacted]

I have attached copies of the Magistrate's decision as well as DOJ's final Memorandum of Law in support of the appeal.

DOJ's Final emorandum of Law

Magistrate's decision (WDPA).p...

b3
b5
b7E

[redacted]

[redacted]

[redacted]

[redacted]Case table.doc

[redacted]

CELL/OTD 008360

If you have any questions regarding the above, please let me know. AGC [redacted] STLU, and AGC [redacted] ILU, are also available to address any questions you may have.

b6
b7C

[redacted]
Section Chief
Science and Technology Law Office
Office of the General Counsel
HQ: [redacted]
Chantilly: [redacted]
bb: [redacted]
PRIVILEGED DELIBERATIVE DOCUMENT - NOT FOR DISCLOSURE OUTSIDE THE FBI WITHOUT PRIOR OGC APPROVAL

UNCLASSIFIED

UNCLASSIFIED

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

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	)	Magistrate's No.: 07-524

GOVERNMENT'S MEMORANDUM OF LAW
IN SUPPORT OF REQUEST FOR REVIEW

AND NOW comes the United States of America by its attorneys, Mary Beth Buchanan, United States Attorney for the Western District of Pennsylvania, and Soo C. Song, Assistant United States Attorney for said district, and hereby seeks review of the Opinion and Memorandum Order entered on February 19, 2008, by United States Magistrate Judge Lisa Pupo Lenihan at Magistrate's No. 07-524M, denying an application by the United States seeking disclosure of historical cell-site information pursuant to Sections 2703(c) & (d) of the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(c) & (d) (the "Opinion and Order").[1] Copies of the Application and the Opinion and Order are attached as Exhibits A (filed separately under seal) and B, respectively. For the reasons set forth below, the government respectfully submits that this Court should reverse the Magistrate Judge's order and grant the Application in the instant case.

I. FACTUAL AND PROCEDURAL HISTORY

A. Historical Cell-Site Information

Cellular telephone companies keep, in the regular course of their business, records of certain

[1] The Opinion and Order has since been published as *In re Application of the United States*, 534 F. Supp. 2d 585 (W.D. Pa. 2008). Although authored by Magistrate Judge Lenihan, the Opinion and Order was signed by all but one of the Magistrate Judges in this district.

information associated with their customers' calls. Exhibit C contains an exemplar of these records from a major carrier, Sprint-Nextel, the same carrier whose records are at issue in the present case.[2] As reflected in Exhibit C, the records include for each call a customer made or received: (1) the date and time of the call; (2) the telephone numbers involved; (3) the cell tower to which the customer connected at the beginning of the call; (4) the cell tower to which the customer was connected at the end of the call; and (5) the duration of the call. The records may also, but do not always, specify a particular sector of a cell tower used to transmit a call.[3] No such record is created when the phone is not in use.

Cell tower information is useful to law enforcement because of the limited information it provides about the location of a cell phone when a call is made. As one court has explained:

> The information does not provide a "virtual map" of the user's location. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas.

In re Application of United States for an Order for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (citation omitted). No Global Positioning System ("GPS"), that is, satellite-derived data, or other precision location information is contained in the historical records provided pursuant to the requested orders. Indeed, cell-site records do not even indicate a phone's distance from the serving tower, let alone its specific location.

---

[2] Because these records contain sensitive information pertaining to a recent investigation, certain identifying information – the telephone numbers involved – has been redacted.

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

B. The United States' Application Pursuant to 18 U.S.C. § 2703(d) in this Investigation

Pursuant to 18 U.S.C. § 2703(c)(1), the United States may require a provider of electronic communication service 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 court order for such disclosure pursuant to 18 U.S.C. § 2703(d) (hereinafter, a "2703(d) order"). A 2703(d) order is issued by a court when the government provides "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

On February 22, 2008, the United States filed an application with Magistrate Judge Lenihan seeking a 2703(d) order directing Sprint Spectrum to disclose certain historical connection and cell-site information associated with a specified cell phone. *See* Exhibit A. The cell phone records are relevant and material to an ongoing investigation into large-scale narcotics trafficking and various related violent crimes.

In June 2007, the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") learned from a confidential source that a particular subject and his associates use their wireless telephones to arrange meetings and transactions in furtherance of their drug trafficking activities. Additional investigation, along with information from the source, indicates that the subject's narcotics supplier lives in another state. Because the subject and his confederates use a variety of vehicles and properties to conduct their illegal activities, physical surveillance has proven difficult. In order to develop better information on the location and identity of the drug supplier, the instant Application seeks historical cell-site records concerning a phone known to be used by the subject. Section

2703(d) orders are broadly used and widely accepted for these types of purposes in federal criminal investigations across the country.

On February 19, the Magistrate Judge denied the Application, ruling in a written opinion that the United States is barred as a matter of law from obtaining historical cell-site information pursuant to a 2703(d) order.

II. ISSUE PRESENTED

The issue before the Court is purely a question of law, namely whether the government may obtain historical cell-site usage records pursuant to an order under 18 U.S.C. § 2703(d).

III. SUMMARY OF ARGUMENT

Section 2703(d) permits the government to obtain a court order compelling historical cell-site usage information from a wireless carrier. The plain language of the statute unambiguously states that the government may require "a provider of electronic communication service" to disclose "a record or other information pertaining to a subscriber" pursuant to a 2703(d) order. As explained below, historical cell-site information satisfies each element of the statute, a position endorsed in recent months by several other courts.

In reaching the opposite conclusion, the Opinion and Order contains numerous errors, both as to the facts of the underlying technology and as to the interpretation of applicable law. Indeed, as discussed below, we believe the Opinion and Order materially relies on at least one statute (and several cases) wholly inapplicable to the government's request for stored records of past customer activity. In addition, because wireless carriers regularly generate and retain the records at issue, and because these records provide only a very general indication of a user's whereabouts at certain times

in the past, the requested cell-site records do not implicate a Fourth Amendment privacy interest. Because the Opinion and Order misstates both the relevant facts and the applicable law, we respectfully urge the Court to reverse.

IV. ARGUMENT

A. Historical Cell-Site Information Falls Within the Scope of Sections 2703(c) and (d)

As the Third Circuit has often reiterated, "'[t]he plain language of the statute is the starting place in our inquiry.'" *United States v. Introcaso*, 506 F.3d 260, 264 (3d Cir. 2007) (*quoting Staples v. United States*, 511 U.S. 600, 605 (1994)). "'If the language of a statute is clear[,] the text of the statute is the end of the matter.'" *Id.* (*quoting United States v. Jones*, 471 F.3d 478, 480 (3d Cir. 2006)).

The Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.*, establishes a comprehensive framework regulating government access to customer records in the possession of communication service providers. The statute's structure reflects a carefully crafted series of Congressional judgments; it distinguishes not only between communications contents (§ 2703(a), (b)) and non-content records (§ 2703(c)), but also between different classes of non-content records.

18 U.S.C. § 2703 unambiguously states that the government may require "a provider of electronic communication service" to disclose "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)" pursuant to a 2703(d) order.[4] *See* 18 U.S.C. § 2703(c)(1). As explained below, cell-site information quite

[4] As noted above, a 2703(d) order is issued by a court when the government provides "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are

clearly satisfies each of the three elements necessary to fall within the scope of this provision.

First, a cell phone company is a provider of electronic communication service. "Electronic communication service" is defined to mean "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. §§ 2510(15) & 2711(1). Cell phone service providers provide their customers with the ability to send wire communications, and thus they are providers of electronic communication service. *See* 18 U.S.C. § 2510(1) (defining wire communications).

Second, cell-site information constitutes "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." Historical cell-site information is a record stored by the provider concerning the particular cell tower used by a subscriber to make a particular cell phone call, and it is therefore "a record or other information pertaining to a subscriber or customer." *See In re Application of United States for an Order for Disclosure of Telecommunications Records*, 405 F. Supp.2d 435, 444 (S.D.N.Y. 2005) (noting that cell-site data is "information" and "'pertain[s]' to a subscriber...or customer of cellular telephone service").

Third, cell-site information is non-content information, as it does not provide the content of any phone conversation the user has over the cell phone. *See* 18 U.S.C. § 2510(8) (defining the "contents" of a communication to include information concerning its "substance, purport, or meaning"). Thus, because historical cell-site information satisfies each of the three elements of § 2703(c)(1), its disclosure may be compelled pursuant to 2703(d) order.

While the statute is unambiguous and thus resort to the legislative history is unnecessary, the

---

relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

legislative history of § 2703(c)(1) nevertheless confirms that it encompasses cell-site information. When the SCA was first enacted as part of the Electronic Communications Privacy Act ("ECPA") in 1986, it permitted disclosure pursuant to a 2703(d) order (or subpoena) of the same catch-all category of "record[s] or other information pertaining to a subscriber or customer of such service (not including the contents of communications)" now codified at 18 U.S.C. § 2703(c)(1). *See* ECPA § 201, P.L. 99-508, 100 Stat. 1848, 1862 (1986). The accompanying 1986 Senate report emphasized the breadth of the "record or other information" category of information: "the information involved is information about the customer's use of the service[,] not the content of the customer's communications." S. Rep. No. 541, 99th Cong., 2d Sess. 38 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3592 (1986). Moreover, cellular telephones were one of the new technologies of particular importance to Congress when it enacted ECPA, so there is no basis to exclude cellular telephone usage records from the scope of § 2703. *See* H.R. Rep. No. 647, 99th Cong., 2d Sess. 20-21 (1986).

Numerous recent decisions confirm the government's view that 2703(d) orders may be used to obtain historical cell-site records. For instance, in September 2007, United States District Court Judge Stearns in Boston reversed a magistrate judge's denial of a 2703(d) application for such records. *See In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007) ("*Stearns D. Mass. Opinion*"). After conducting a careful analysis of the SCA's text, Judge Stearns held that "historical cell site information clearly satisfies" the statute's definitional requirements, rejecting the magistrate's analysis and granting the application. *Id.* at 80.

The following month, Judge Rosenthal in Houston confronted a similar situation: a magistrate judge had denied the government's application for, *inter alia*, historical cell-site data

under the authority of § 2703(d). *See In re Application*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007). Here, too, the district court found the magistrate's objections on this question wholly without merit, reversing and holding that "the Government's request for historical cell-site information is within the statutory authorization." *Id.* at *5.

And most recently, on March 26, 2008, a federal magistrate judge in Atlanta issued an opinion rejecting a defendant's motion to suppress historical cell-site records acquired by means of a 2703(d) order. *See United States v. Suarez-Blanca*, No. 1:07-CR-0023-MHS/AJB (N.D. Ga. Mar. 26, 2008) (copy attached as Exhibit D). In his opinion endorsing the government's approach, the magistrate noted – and disagreed with – the Magistrate Judge's Opinion and Order in the present case. *Id.* at 32-33.

B. No Other Authority Limits the Compelled Disclosure of Historical Cell-Site Information Pursuant to a 2703(d) Order

The Opinion and Order errs at the outset by proposing to answer a legal question that is simply not relevant to this case. Instead of addressing the question at hand – whether the government may obtain historical cell-site records via a 2703(d) order – the decision below places a great deal of emphasis on determining the proper authority for obtaining such information prospectively. Prospective cell-site information is not at issue in this case. The decision never fully recovers from this initial wrong turn, and as a result conflates the legal principles actually relevant to the government's Application.

In the course of the analysis, the Magistrate Judge cites several authorities as purported limits on the government's ability to compel disclosure of historical cell-site information pursuant to 2703(d) orders. In particular, the Opinion and Order concludes that 47 U.S.C. § 1002(a)(2); the

mobile tracking device provision of 18 U.S.C. § 3117; the text of § 2703 itself; the Fourth Amendment; and the Wireless Communication and Public Safety Act of 1999 ("WCPSA") all bar the government from compelling disclosure of cell-site information via 2703(d) orders.

However, as explained below, the cited Title 47 provision applies only to prospective evidence-gathering, and not to the instant Application for an order compelling historical records. Section 3117 is likewise inapplicable because a user's own phone is not a "tracking device" within the narrow meaning of that statute. On the other hand, § 2703 not only applies, but on its face permits the government's current Application. Finally, the customer records at issue are not protected by the Fourth Amendment. As a result, none of these authorities prohibits or even limits compelled production of historical cell-site information pursuant to a 2703(d) order, and the Opinion and Order below should therefore be reversed.

1. 47 U.S.C. § 1002 Does Not Apply to Requests for Historical Records, and Therefore Does Not Prohibit Compelled Production of Historical Cell-Site Information Pursuant to a 2703(d) Order

The Opinion and Order below devotes enormous space to discussion of the 1994 Communications Assistance for Law Enforcement Act (CALEA). In particular, the decision below places great weight on the fact that CALEA, at 47 U.S.C. § 1002(a)(2), states that

> information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code) ... shall not include any information that may disclose the physical location of the subscriber.

(Emphasis supplied.) However, the present Application neither invokes nor in any way relies on the pen register/trap and trace statute. On the contrary, the government's request – for historical, not future, cell-site records – relies on the entirely separate authority of 18 U.S.C. § 2703(d).

Because the CALEA provision quoted above mentions only the pen/trap statute, and not

§ 2703(d), it would be wholly improper to read into it what Congress chose to omit. Under the longstanding canon of *expressio unius est exclusio alterius* ("the expression of one is the exclusion of the other"), a court should presume that if "Congress wanted to include such a requirement ... it knew exactly how to do so." *United States v. Thornton*, 306 F.3d 1355, 1359 (3d Cir. 2002). In the case of CALEA, this omission can hardly be called accidental. Congress was well aware of § 2703(d) in its deliberations over CALEA; in fact, a separate portion of the Act amended § 2703(d) to raise the showing required of the government. *See* Pub. L. 103-414, § 207(a) (1994).[5]

The decision below simply disregards the fact that 47 U.S.C. § 1002 imposes limits only on the pen/trap statute, and not on § 2703(d). Instead, it leans heavily in its analysis on numerous cases applying the CALEA restriction to government requests for prospective collection of future cell-site records.[6]

---

[5] Nor does *expressio unius* produce an absurd result in this instance. A pen register order may issue where the government has made a mere certification of relevance. *See* 18 U.S.C. § 3123(a)(1). In contrast, § 2703(d) imposes the higher "specific and articulable facts" criterion. *See* H. Rep. No. 827, 103d Cong., 2d Sess. 31 (1994) (noting that change in required 2703(d) showing from relevance to specific and articulable facts "rais[es] the standard"), *reprinted in* 1994 U.S. Code Cong. & Admin. News 3489, 3511.

[6] Magistrates and district courts have disagreed over whether § 2703 and the pen register statute can be used together to compel disclosure of cell-site information prospectively, an issue not raised in this case. *Compare In re Application of United States for an Order for Prospective Cell Site Location Information*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (upholding "hybrid" use of 2703(d) orders and pen/trap statute to compel prospective disclosure of cell-site information) *with In re Application of United States for an Order Authorizing Use of a Pen Register and Trap and Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (rejecting such hybrid orders).

However, as the Magistrate Judge's Opinion and Order concedes, *see* 534 F. Supp. 2d at 600, even judges who have rejected prospective hybrid orders for cell-site information have agreed that compelled disclosure of historical cell-site information pursuant to 2703(d) orders is proper. *See, e.g.*, 396 F. Supp. 2d at 327 ("The applicable statutes allow the government to obtain historical cell site information on the basis of a showing less exacting than probable cause, but do not allow it to obtain such information prospectively on a real-time basis.").

The Magistrate's opinion acknowledges the prior decisions holding (or implying) that historical cell-site records may be obtained by way of § 2703(d). In the same breath, however, the decision below dismisses that same precedent with the surprising claim that the legal distinction between prospective and historical cell-site records is "largely-unexplained." 534 F. Supp. 2d at 603. In fact, the government submits that the distinction is indeed clear, depending as it does on the explicit wording and structure of the pertinent statutes.

In crafting the federal statutes regulating governmental access to telecommunications records, Congress has unambiguously distinguished between historical (stored) and future records. Most prominently, Chapter 121 of Title 18 (the Stored Communications Act, §§ 2701 *et seq.*) stands in contrast to the Wiretap Act (Chapter 119) and the pen register statute (Chapter 206), both of which exclusively regulate prospective, ongoing surveillance (of content and non-content, respectively). Thus, the mechanism for obtaining historical telephone calling records – a subpoena, as provided for at § 2703(c)(2)(C) – differs from the authority under the pen/trap statute for monitoring the telephone numbers of future calls to or from a target telephone.

The decision below improperly disregards this key aspect of the statutes. Because it wrongly relies on the CALEA limitation (and cases applying it) to conclude that the statutes "do not distinguish between historic[al] and prospective [cell-site records]," 534 F. Supp. 2d at 586 n.4, its analysis should be rejected.

2. The Statutory Provisions Concerning "Tracking Devices" Do Not Limit Compelled Disclosure of Historical Cell-Site Information

The Opinion and Order also asserts that the United States may not use a 2703(d) order here because historical cell-site information is a communication from a "tracking device" as defined in

18 U.S.C. § 3117. *See* 534 F. Supp. 2d at 601-07. The analysis, however, is simply not supportable. As explained below, "tracking device" communications are excluded only from the definition of "electronic communication"; cellular telephone calls are instead "wire communications," a defined term with no comparable exclusion. Second, a user's own wireless phone is not a "tracking device" within the narrow meaning of the statute.

The decision below relies heavily on 18 U.S.C. § 2510(12)(C), which excludes "any communication from a tracking device" from the definition of "electronic communication." Under the reasoning of the Opinion and Order, this provision excludes cell-site records from the reach of ECPA. In reaching this conclusion, however, the opinion overlooks one crucial, plainly expressed statutory distinction: cellular telephone calls are not "electronic communications" under any circumstances. On the contrary, conventional cellular calls are instead "wire communications" as defined at section 2510(1).[7] Of equal importance, the "wire" and "electronic" categories are mutually exclusive: a "wire communication" cannot, under the express terms of the statute, also be an "electronic communication." *See* § 2510(12)(A) (""electronic communication' ... does not include–(A) any wire or oral communication"). Thus, properly analyzed under the statute, historical cell-site information concerning a wireless telephone call is plainly "a record or other information pertaining to a subscriber" using a service provider's network to send and receive "wire communications." *See Stearns D. Mass. Opinion*, 509 F. Supp. 2d at 80 (reversing magistrate

[7] The essential distinction is that a "wire communication" necessarily involves the human voice. *See* § 2510(1) (defining "wire communication") and § 2510 (defining "aural transfer"); S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3565 ("cellular communications – whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone – are included in the definition of 'wire communications' and are covered by the statute").

judge's contrary conclusion).

The decision below overlooks these clearly articulated distinctions. Instead, the opinion dwells at length on the definition of an inapposite term ("electronic communication"). Having done so, the Opinion and Order further distorts the statute by construing the clear phrase "record or other information pertaining to a subscriber" to exclude

> information that is regarding or derived under a service (*e.g.*, a tracking capability/function) that may be used to facilitate the provision of an electronic communication service (*e.g.*, the transmission of voice/text material), but that is not *itself* an electronic communication service (as, *e.g.*, by definition).

534 F. Supp. at 604 (footnote omitted). Because this unduly complicated interpretation – unsupported by even a single citation to the legislative history of the statute – does violence to the plain meaning of "pertaining to," this Court must reject it. *See Malloy v. Eichler*, 860 F.2d 1179, 1183 (3d Cir. 1988) ("Where the language of the statute is clear, only 'the most extraordinary showing of contrary intentions' justify altering the plain meaning of a statute.") (*quoting Garcia v. United States*, 469 U.S. 70, 75 (1984)).

In addition, the decision below errs in finding that the target cell phone was a "tracking device" within the meaning of 18 U.S.C. § 3117. This overly expansive reading runs contrary to the language, structure, and legislative history of ECPA, and it would significantly undermine privacy protections for users of communication networks.

The structure of 18 U.S.C. § 3117 makes clear that a "tracking device" is a homing device installed by the government. Specifically, 18 U.S.C. § 3117(a) applies only when a court is authorized to issue an order "for the installation of a mobile tracking device." It then provides that "such order may authorize the use of that device within the jurisdiction of the court, and outside that

jurisdiction if the device is installed in that jurisdiction." *Id.* Thus, the purpose of the tracking device statute is to provide a court with extra-territorial jurisdiction over use of tracking devices installed within its jurisdiction. Given the limited purpose of the tracking device statute, there is no basis for interpreting "tracking device" broadly to encompass devices which the government would never have any reason to apply to a court to install or use. *See Stearns D. Mass. Opinion*, 509 F. Supp. 2d at 81 n.11 (§ 3117 "governs the 'installation' of tracking devices. The 'tracking' of a cell phone does not require the installation of any sort of device."); *In re Application*, 405 F. Supp. 2d 435, 449 n.8 (S.D.N.Y. 2005) (same).

The legislative history of § 3117 is equally clear that "tracking devices" are homing devices, not cell phones or other communications technologies. Most obviously, the 1986 House Report on ECPA cites the two landmark Supreme Court decisions concerning "beeper" homing devices, *United States v. Knotts*, 460 U.S. 276 (1983) (beeper installed in can of chloroform and used to track movements of car) and *United States v. Karo*, 468 U.S. 705 (1984) (beeper installed in can of ether expected to be used in production of cocaine). No mention is made of cellular telephones.

Likewise, the Senate Report on ECPA includes a glossary of technological terms. The glossary, which defines electronic tracking devices separately from cell phones and pagers, defines "electronic tracking devices" as follows:

> These are 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. 541, 99th Cong., 2d Sess. 10 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin.

News 3555, 3564 (1986).

Even more revealing is the fact that the very same 1986 legislation[8] addresses cellular telephone technology extensively in numerous other provisions unrelated to "tracking devices." Congress enacted ECPA because the Wiretap Act "had not kept pace with the development of communications and computer technology." S. Rep. No. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3556 (1986). Cellular phones were one of the new technologies of particular importance to Congress, *see id.* at 2 & 9, and cellular technology is central to much of ECPA's legislative history. *See id.* at 2, 4, 6-9, 11-12, 21, & 29-30.

Congress made clear that cellular communications were to be protected as wire communications by the Wiretap Act and the SCA. In particular, Congress amended the definition of "wire communication" to ensure that it encompassed cellular communications by inserting the phrase "including the use of such connection in a switching station" into 18 U.S.C. § 2510(1). *See* ECPA § 101, Pub. L. No. 99-508, 100 Stat. 1848 (1986). As noted by the Senate Report on ECPA, "[t]his subparagraph makes clear that cellular communications--whether they are between two cellular telephones or between a cellular telephone and a 'land line' telephone--are included in the definition of 'wire communications' and are covered by the statute." S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3565 (1986).

Despite this extensive discussion of cell phones throughout ECPA's legislative history, there is not a scintilla of evidence in the legislative history that Congress intended cell phones to be classified as tracking devices. Instead, all discussion of tracking devices suggests that Congress

---

[8] The tracking device statute was enacted as part of ECPA. *See* Pub. L. No. 99-508, 100 Stat. 1848, § 108 (1986).

understood tracking devices to be homing devices installed by the government.

There is no reason to supply "tracking device" with a meaning much broader than that intended by Congress, especially because doing so would deny many communications the privacy protection Congress intended them to have. If cell phones were classified as "tracking devices," text messages or e-mail transmitted from them would not be "electronic communications" under 18 U.S.C. § 2510(12)(C). As a result, such communications would fall outside the scope of the Wiretap Act, and it would no longer be a federal crime for an eavesdropper to intercept them. *See* 18 U.S.C. § 2511(1)(a) (criminalizing interception of wire, oral, and electronic communications). This result is plainly contrary to Congress's purposes in passing ECPA, and the Opinion and Order's expansive interpretation of "tracking device" should therefore be rejected.

Moreover, if "tracking device" were given the broad interpretation adopted below, nearly all communications devices would be tracking devices. Certainly any device relying on the cellular communication system (including many pagers, text messaging devices such as Blackberries, and cellular Internet systems) would be a "tracking device." The same is also true of banking ATMs, retail credit-card terminals, or even landline telephones (since it is possible to determine information about a person's location from his use of each). But the Magistrate Judge's reasoning extends much further. It is generally possible to determine the physical location of a user connected to the Internet, and the whereabouts of fugitives and other suspects are frequently discovered based on their use of Internet-connected computers. Treating all such devices as "tracking devices" grossly distorts § 3117's scope and purpose, and this Court should reject the Magistrate Judge's overly broad reading of the statute. *See United States v. Schneider*, 14 F.3d 876, 880 (3d Cir. 1994) (a court has an obligation to construe statutes to avoid absurd results).

A recent opinion from the Eastern District of California underscores all of these points:

> No use of cell phones and cell towers for tracking was expressly contemplated, and perhaps was not even possible in 1986. Certainly the legislative history gives no such indication.
>
> In addition, it would prove far too much to find that Congress contemplated legislating about cell phones as tracking devices. For example, if an agent presently used a cell phone to communicate the whereabouts of a suspect by using the phone's video feature while he was surveilling the suspect, one could fit this situation into the words of the statute-one was using an electronic device which "permitted" the tracking of the suspect. Or, take the example of the ubiquitous monitoring cameras, such as the "red light," parking lot or freeway cameras. These cameras track the location of many persons, albeit in a confined location, and could also fit in with the words of the statute. It is best to take the cue from Congress in this respect of electronic tracking devices, and confine § 3117(b) to the transponder type devices placed upon the object or person to be tracked.

In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007).

Thus, even if it were the case that cellular telephone calls were "electronic communications" – as set forth above, they unquestionably are not – the "tracking device" exclusion from the definition of that term is irrelevant because a user's own phone falls outside the narrow scope of that defined term.[9] For this reason as well, the decision below should be reversed.

---

[9] The Opinion and Order asserts that the use of tracking devices pursuant to 18 U.S.C. § 3117 requires probable cause. 534 F. Supp. 2d at 595. Even if a subscriber's own cell phone were a "tracking device," it would not follow that a Rule 41 warrant founded on a showing of probable cause would be required to obtain historical cell-site records. First, as the Advisory Committee Notes to the 2006 amendments to Rule 41 explain, if "officers intend to install and use the [tracking] device without implicating any Fourth Amendment rights, there is no need to obtain the warrant." Fed. R. Crim. P. 41, Advisory Comm. Notes to 2006 Amendments, Subdivision (b). The Committee Notes further explain that "[t]he tracking device statute, 18 U.S.C. § 3117, does not specify the standard an applicant must meet to install a tracking device." *Id.* at subdivision (d).

Indeed, the statute does not even prohibit the use of a tracking device in the absence of conformity with § 3117. *See United States v. Gbemisola*, 225 F.3d 753, 758 (D.C. Cir. 2000) ("But by contrast to statutes governing other kinds of electronic surveillance devices, section 3117 does not prohibit the use of a tracking device in the absence of conformity with the

3. Section 2703(d) Does Not Permit a Court to Demand a Showing of Probable Cause

The Opinion and Order also asserts that § 2703 permits a court to demand a showing of probable cause as a precondition to issuance of a 2703(d) order. This conclusion allegedly flows from the express language and structure of § 2703. Instead, the text of the statute points to the opposite reading.

As before, "every exercise of statutory interpretation begins with an examination of the plain language of the statute." *Rosenberg v. XM Ventures*, 274 F.3d 137, 141 (3d Cir. 2001). Where statutory language is "plain and unambiguous," no further inquiry is necessary. *Id.* On its face, § 2703(d) demands a showing of "specific and articulable facts." Nowhere does that subsection state, or even imply, that probable cause is or may be demanded.

Section 2703(c) permits the government to use any of various methods to obtain stored, non-content customer records. As the House Judiciary Committee noted in its report accompanying ECPA in 1986,

> the government must use one of three sets of authorized procedures. The government can rely on administrative subpoenas or grand jury subpoenas to the extent that such processes are legally authorized. Alternatively, the government can use a search warrant. Finally, the government can seek a court order directing the disclosure of such records. If a court order is sought then the government must meet the procedural requirements of subsection (d).

H. Rep. No. 647, 99th Cong, 2d Sess. 69 (1986) (emphasis added). Current § 2703(c)(1) preserves this structure, explicitly making 2703(d) orders a means of compelling records separate from and alternative to a warrant based on probable cause. *Compare* § 2703(c)(1)(A) (authorizing use of search warrant under Rule 41) *with* § 2703(c)(1)(B) (authorizing use of 2703(d) court order).

---

section.") (emphasis in original); *In re Application*, 405 F. Supp. 2d at 449 n.8 (same).

To do as the Magistrate Judge did below, and insist that a § 2703(d) application set forth probable cause, is in effect to demand a warrant, and thus to render part of the statute superfluous. This contravenes the longstanding canon that a court should, whenever possible, give effect to every provision of a statute. *See, e.g., Tavarez v. Klingensmith*, 372 F.3d 188, 190 (3d Cir. 2004).

Even if the text of the statute were not clear on its face, an examination of the legislative history confirms Congress's intent that a 2703(d) court order be granted on less than probable cause. As originally enacted in 1986, § 2703(d) required only a showing that "there is reason to believe ... the records or other information sought, are relevant to a legitimate law enforcement inquiry." Pub. L. 99-508, § 201 (1986). Eight years later, Congress affirmatively chose to raise the test to the current "specific and articulable facts" standard. *See* Pub. L. 103-414, § 207(a) (1994). As the accompanying House Judiciary Committee report makes clear, this is "an intermediate standard ... higher than a subpoena, but not a probable cause warrant." H. Rep. No. 827, 103d Cong., 2d Sess. 31 (1994) (emphasis added), *reprinted in* 1994 U.S. Code Cong. & Admin. News 3489, 3511.

4. The Fourth Amendment Does Not Bar Compelled Disclosure of Historical Cell-Site Information Pursuant to a 2703(d) Order

Finally, the Opinion and Order suggests that a user has a reasonable expectation of privacy in historical cell-site information. 534 F. Supp. 2d at 610-11. This conclusion is incorrect for two distinct reasons. First, under the established principles of *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), there is no reasonable expectation of privacy in such information, and, accordingly, no Fourth Amendment-protected privacy interest. Second, historical cell-site information is far too imprecise by any measure to intrude upon a reasonable expectation of privacy. Thus, the Fourth Amendment does not limit disclosure of historical cell-site

information pursuant to 2703(d) orders.

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

The Court's reasoning in *Smith v. Maryland* leads to the same result. In *Smith*, the Court held both that telephone users had no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. *See Smith*, 442 U.S. at 742-44. The Court's reasoning applies equally to cell-site information. First, the

Court stated: "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. Similarly, cell phone users understand that they must send a radio signal which is received by a cell phone company's antenna in order to route their call to its intended recipient. (Indeed, cell phone users are intimately familiar with the relationship between call quality and radio signal strength, as typically indicated by a series of bars on their phones' displays.)

Second, under the reasoning of *Smith*, any subjective expectation of privacy in cell-site information is unreasonable. In *Smith*, the Court explicitly held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." *Id.* at 743 (internal quotation omitted). It noted that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. In *Smith*, the user "voluntarily conveyed numerical information to the telephone company" and thereby "assumed the risk that the company would reveal to the police the numbers he dialed." *Id.* at 744. Here, a cell phone user transmits a signal to a cell tower for his call to be connected and thereby assumes the risk that the cell phone provider will reveal the cell-site information to law enforcement. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no expectation of privacy in cell-site information.

As a business record in the possession of a third party, cell-site information should not be judged under Fourth Amendment standards for transponders and similar tracking devices surreptitiously installed by the government. However, even measured against the constitutional

standards articulated by the Supreme Court in this area, there is no reasonable expectation of privacy in cell-site information. The mere use of a tracking device, even when surreptitiously placed by the government, does not implicate Fourth Amendment privacy concerns. *See United States v. Knotts*, 460 U.S. 276, 282 (1983) (police monitoring of beeper signals along public roads did not invade any legitimate expectation of privacy). To be of constitutional concern, a surreptitiously installed tracking device must reveal facts about the interior of a constitutionally protected space. *See United States v. Karo*, 468 U.S. 705, 713 (1984) (distinguishing *Knotts* and holding that police monitoring of a beeper that disclosed information about the interior of a private residence, not open to visual surveillance, required a warrant).

The Opinion and Order's "Technological Development Overview" makes certain claims about wireless telephone location information: 1) that wireless phone companies "store cell tower registration histories" reflecting a phone's location at seven-second intervals; 2) that "the location of just the nearest tower itself can place the phone within approximately 200 feet"; and 3) that triangulation techniques or GPS capabilities make a user's location "precisely determinable" to within as little as 50 feet. 534 F. Supp. 2d at 589-90. The first two claims are demonstrably false, and the third claim (also incorrect) is irrelevant to the separate type of records sought in the instant Application.

On the first issue, the Opinion and Order is correct that a wireless phone, when first powered on, "registers" with a nearby tower, and that the phone thereafter periodically re-registers with the network over time. (Network awareness of a phone's approximate recent whereabouts makes delivery of incoming calls more efficient.) However, no "history" of these events is maintained: once a phone moves into the coverage area of a new tower and registers with it, the prior information

is no longer useful, and the network management software simply deletes the prior registration data. Put differently, the only "registration" data in a carrier's possession at any given moment is the current information. No tower registration history is kept.

As Exhibit C makes clear, historical cell-site data retained by the carriers – that is, the category of information called for by the government's Application in this case – reflects only the identity of the serving tower (and sector, if applicable) when the phone is in active use. The carrier recorded and preserved the cell-site information only at the start and end of actual telephone calls occurring over a few days. Plainly, a typical record such as Exhibit C does not even reveal the location of a nearby cell tower – let alone the phone user's own location – at 7-second intervals.

In making the second claim, the Opinion and Order cites only to a single law student note, which says

> [a] very general sense of a phone's is [*sic*] can be gathered by tracking the location of the tower being used during a call. In urban areas, where there are many towers, this may give a picture location [*sic*] within a couple hundred feet. In rural areas, towers may be miles apart. A slightly more accurate location picture can be generated by tracking which 120 degree "face" of the tower is receiving a cell phone's signal.

Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 Hastings Comm. & Ent. L.J. 421, 426-27 (Spring 2007). The author's sole source for these claims is a recent decision, *In re Application of United States for an Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005), which in fact contradicts the key assertion about precision in urban settings:

> In suburban or rural areas, towers can be many miles apart. The Court has examined a map of cellular towers of a provider in lower Manhattan, which is one of the areas more densely populated by towers. In this area, the towers may be anywhere from several hundred feet to as many as 2000 feet or more apart.
>
> [...]

> The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas.

Id. at 437 & 449 (expressly rejecting claim that Fourth Amendment protects such general location information) (emphasis added).

The Opinion and Order's second claim also contradicts repeated findings of the Federal Communications Commission, which relies on the advice of skilled telecommunications engineers (both on FCC staff and those employed by carriers filing public comments). In one proceeding, for instance, the FCC found that a certain location-finding technique accurate to within 500-1000 meters (roughly 1640-3280 ft.) "would be significantly more precise" than "the location of the cell site or sector receiving the call." *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000).[10] The Commission went on to note that simple cell-site information "can in some instances be misleading, as wireless calls are not always handled by the nearest cell." *Id.*

Given a stark choice between crediting a lone law student (in this case, one misstating the factual findings of a federal court) and the FCC, the government respectfully suggests to this Court that the FCC is more credible. For the same reasons, the Opinion and Order's claim that historical cell-site records "place the phone within approximately 200 feet" should also be rejected.

---

[10] *See also In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 16 FCC Rcd. 18305, 18311 n.49 (Oct. 12, 2001) (similar technique to locate phone within a 1000-meter radius held to be "a notable improvement in accuracy and reliability over ... the location of the cell site or sector receiving the call."); *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 14 FCC Rcd. 17388, 17414 (Oct. 6, 1999) (accuracy of 285 meters – 311 feet – "would be far more accurate than ... cell site location information.") (emphasis added).

The Opinion and Order's third claim – that triangulation techniques or GPS capabilities currently make a user's location "precisely determinable" to within as little as 50 feet – is simply inapposite.[11] Those entirely distinct techniques relate to real-time (or prospective) location-finding capabilities, "Enhanced 9-1-1 Phase II" in FCC parlance. As noted explicitly in all of the FCC documents referenced above, these prospective location-finding capabilities have been imposed by the FCC for the very reason that cell-site data ("Phase I" information) is so imprecise.

Simply put, the government's present Application seeks only historical cell-site – that is, single-tower and sector – records. It does not seek GPS or "triangulation" information, which is in any event almost never available for past time periods.[12] Rather, the government has requested only the type of records shown in Exhibit C.

As an example, the first line of Exhibit C shows a May 1, 2007 call in the Boston area, Location Area Code 4361, from Cell ID 49874. A separate spreadsheet (supplied by the carrier) that contains only general information about tower attributes – that is, no information about specific customer activities or usage – reveals that Cell ID 49874 corresponds to face number 1 (of 3) on a

---

[11] As an aside, the government notes that this is also an exaggeration. Current FCC regulations for emergency (911) calls require that, by September 11, 2012 – more than four years hence – carriers be able to deliver location data at a level of 100 meters for 67 percent of calls and 300 meters for 95 percent of calls (for so-called "network-based" solutions), and 50 meters for 67 percent of calls and 150 meters for 95 percent of calls (for handset-based solutions). *See* 47 C.F.R. § 20.18(h)(1)(i), (ii). These requirements apply only to customer-initiated calls to a "public safety answering point" (911 operators). Moreover, the deadline for regulatory compliance has been delayed repeatedly in recent years, in large part because of carrier opposition or non-compliance.

[12] Carriers do not typically generate and retain more precise location records in the normal course. The exceptions to this general rule are so-called "kiddie tracker" phones, where – for a separate fee – some carriers offer a service for parents to monitor the movement of a child's phone. *See, e.g.*, http://www.alltel.com/familyfinder . These services are not included in standard feature packages, and are often restricted to certain handsets. *See, e.g., id.*

tower at a particular location north of Boston. Here, this means that the target phone was likely, but not necessarily, roughly northeast of the specified tower coordinates. It does not give the coordinates of the target phone itself, nor even an approximate indication of its distance from the tower; instead it only suggests an area tens of thousands (or more) square yards large in which the target phone was used. As noted above by the FCC, the fact that wireless calls are not always handled by the nearest cell further contributes to the generality and imprecision of this information.

Thus, cellular phone companies' historical records of cell-site usage are much too imprecise to tell whether calls have been made or received from a constitutionally protected space, let alone to reveal facts about the interiors of private homes or other protected spaces. *See* 405 F. Supp. 2d at 449 (cell-site information "does not provide a 'virtual map' of the user's location.... The information does not pinpoint a user's location within a building.").

As a final basis to support the notion that customers enjoy Fourth Amendment rights in the routine business records of their wireless providers, the Opinion and Order cites a range of statutes purportedly conferring constitutional rights. For instance, the decision below invokes the Wireless Communication and Public Safety Act of 1999 (WCPSA), 47 U.S.C. § 222(f), asserting that it "expressly recognizes the importance of an individual's expectation of privacy in her physical location." 534 F. Supp. 2d at 610.

In fact, however, the WCPSA offers no such recognition. Instead, the WCPSA simply states that "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information" in certain specified situations. 47 U.S.C. § 222(c)(1)

(emphasis added). The phrase "except as required by law" encompasses appropriate criminal legal process. *See Parastino v. Conestoga Tel & Tel. Co.*, No. Civ. A 99-679, 1999 WL 636664, at *1-2 (E.D.Pa, Aug. 18, 1999) (holding that a valid subpoena falls within the "except as required by law" exception of § 222(c)(1)). Thus, the WCSPA does not create or reinforce any constitutional expectation of privacy, and therefore imposes no bar to the disclosure of cell-site information pursuant to 2703(d) orders.

More importantly, a federal statute cannot in any event establish a constitutional norm. As the Fifth Circuit has observed in analyzing the Right to Financial Privacy Act,

> [w]hile it is evident that Congress has expanded individuals' right to privacy in bank records of their accounts, appellees are mistaken in their contention that the expansion is of constitutional dimensions. The rights created by Congress are statutory, not constitutional.

United States v. Kington, 801 F.2d 733, 737 (5th Cir. 1986) (emphasis supplied).

Thus, because there is no reasonable expectation of privacy in historical cell-site records, the Fourth Amendment does not limit compelled disclosure of such records pursuant to a 2703(d) order.

V. CONCLUSION

For these reasons, the government respectfully submits that this Court should reverse the Opinion and Order below and grant the Application in the instant case.

Respectfully submitted
MARY BETH BUCHANAN
United States Attorney

s/ Soo C. Song
SOO C. SONG
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 644-2645 (Fax)
soo.song@usdoj.gov
DC ID No. 457268

PAUL E. HULL
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 894-7311 (Fax)
paul.hull@usdoj.gov
PA ID No. 35302

MARK ECKENWILER
Associate Director
Office of Enforcement Operations
Criminal Division
U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530

NATHAN JUDISH
Senior Counsel
Computer Crime and Intellectual Property Section
Criminal Division
U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530

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.

Magistrate's No. 07-524M.

United States District Court,
W.D. Pennsylvania.

Feb. 19, 2008.

Background: United States applied for order directing provider of electronic communication services to disclose records to government.

Holding: The District Court, Lenihan, J., held that access to records could not be obtained on simple showing of articulable relevance to ongoing investigation rather than probable cause.

Application denied.

Telecommunications ⇐1475

Stored Communications Act, either alone or in tandem with Pen Registry Statute, does not authorize access to individual's cellular phone-derived location information, either past or prospective, on simple showing of articulable relevance to ongoing investigation rather than probable cause. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. §§ 2703, 3117; Fed.Rules Cr. Proc.Rule 41, 18 U.S.C.A.

Soo C. Song, United States Attorney's Office, Pittsburgh, PA, for Plaintiff.

Before LISA PUPO LENIHAN, SUSAN PARADISE BAXTER, FRANCIS X. CAIAZZA, AMY REYNOLDS HAY and ROBERT C. MITCHELL, United States Magistrate Judges.

OPINION AND MEMORANDUM ORDER

LISA PUPO LENIHAN, United States Magistrate Judge.

I. SUMMATION OF OPINION

The Court writes to express its concerns regarding the Government's *ex parte* applications for cellular telephone ("cell phone") subscriber information from which it may identify an individual's past or present physical/geographic movements/locations not on a showing of probable cause to believe that the information will provide evidence in an investigation premised on a reasonable suspicion of criminal activity, as under the Fourth Amendment,[1] but rather on an articulable, reasonable belief that such information is "relevant to a ... criminal investigation" under the Stored Wire and Electronic Communications and Transactional Records Access statutes (the "Stored Communications Act" or "SCA") alone or in tandem with the Pen Registry Statute (the "PRS").[2] The Court also

1. As discussed *infra*, the Fourth Amendment protects us by providing that the "right of people to be secure in their persons, houses ... against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause." U.S. Const. Amend. IV. The test currently employed to determine whether a search is subject to these Constitutional constraints is taken from Justice Harlan's concurrence in *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), and looks to whether the individual being searched harbors a reasonable expectation of privacy in the object of the search. Where there is a reasonable expectation of privacy, intrusion on that right by the Government for investigatory purposes requires that the Government obtain a warrant by demonstrating to the Court that it has probable cause, *i.e.*, that it make a showing of a fair probability of evidence of criminal activity.

2. The Government's application for cellular telephone information from which it can derive physical location information on the basis of the SCA and PRS read in tandem is re-

writes to set forth its reasons for concluding that, while it recognizes the important and sometimes critical crime prevention and law enforcement value of tracking suspected criminals,[3] the Government's requests for Court Orders mandating a cell phone service provider's covert disclosure of individual subscribers' (and possibly others') physical location information must be accompanied by a showing of probable cause.[4]

The Court emphasizes that the issue is not *whether* the Government can obtain movement/location information, but *only the standard* it must meet to obtain a Court Order for such disclosure and the basis of authority. It emphasizes that the Fourth Amendment standard is not a difficult one, requiring only that the Government support its belief of criminal activity and the probable materiality of the information to be obtained.[5] The Court notes that it is entrusted with the protection of the individual civil liberties, including rights of privacy and rights of free association, so paramount to the maintenance of our democracy. The Court also observes that the location information so broadly sought is extraordinarily personal and potentially sensitive;[6] and that the *ex parte* nature of the proceedings, the comparatively low cost to the Government of the information requested, and the undetectable nature of a CSP's electronic transfer of such information, render these requests particularly vulnerable to abuse.[7] Finally, the Court concludes, from its exhaustive

ferred to as its "hybrid" or "dual authority" theory.

3. *See, e.g., Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators,* 18 Harv. J. Law & Tech., 307, 310 (Fall, 2004) (hereafter *"Who Knows Where You've Been?"*) (discussing criminal cases in which law enforcement's access to cell phone location information may have been critical).

4. The Court recognizes and appreciates that the U.S. Attorney for this District has chosen not to pursue prospective cell tower information without a probable cause affidavit, and accordingly the current application requests only historic cell site location information ("CSLI"); however, the cases considering prospective applications are relevant to this discussion and must be addressed as well. In addition, because this Court concludes that the electronic communications statutes, correctly interpreted, do not distinguish between historic and prospective CSLI, its analysis applies equally to both.

5. The Supreme Court describes probable cause as a "practical, common-sense decision" turning on whether, under the "totality of the circumstances", there is a fair probability that evidence of a crime will be found. *See Illinois v. Gates,* 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983). *Cf. Karo,* 468 U.S. at 717, 104 S.Ct. 3296 (concluding that "Government's contention that warrantless [electronic monitoring] should be deemed reasonable [was] based upon its deprecation of the benefits and exaggeration of the difficulties associated with procurement of a warrant").

6. Location information may reveal, for example, an extra-marital liaison or other information regarding sexual orientation/activity; physical or mental health treatment/conditions (including, *e.g.,* drug or alcohol treatment and/or recovery programs/associations); political and religious affiliations; financial difficulties; domestic difficulties and other family matters (such as marital or family counseling, or the physical or mental health of one's children); and many other matters of a potentially sensitive and extremely personal nature. It is likely to reveal precisely the kind of information that an individual wants and reasonably expects to be private. *Cf. State v. Jackson,* 150 Wash.2d 251, 76 P.3d 217, 223–24 (2003) (noting that the "intrusion into private affairs" from a device producing a record of our travels is "quite extensive").

7. *Cf.* Susan Friwald, *First Principles of Communications Privacy,* 2007 Stan. Tech. L.Rev. 3, 11 (2007) (hereafter *"First Principles"*) (asserting that electronic communications surveillance implicates Fourth Amendment's core concerns because it is (a) hidden, thus requiring greater reliance on the Court's protection of the citizen's interests; (b) and (c)intrusive and continuous, thus requiring higher justification; and (d) indiscriminate, *i.e.,* often

review of the statutes and cases as to both the rapidly-developing law of electronic communications and the Fourth Amendment, together with its extensive review of the legislative history and scholarly commentary, that Congress and the Supreme Court still concur in the principle underlying this Opinion: *i.e.*, that law enforcement's investigative intrusions on our private lives, in the interests of social order and safety, should not be unduly hindered, but must be balanced by appropriate degrees of accountability and judicial review.[8] For these reasons, and notwithstanding the legitimate and significant benefits in law enforcement's ability to obtain information efficiently and effectively, this Court best serves and preserves the fundamental principles underpinning our Constitutional democracy by (1) a careful and thorough parsing of the legislation and (2) a cautious and informed balancing of the competing interests.

Thus, absent express statutory authorization for *ex parte* access to personal movement/location information and/or a precedential/binding interpretative ruling, this Court cannot accede to the Government's request. To the contrary, it must adhere to the canons of statutory construction and read the provisions of the various statutes implicated in a manner that (1) applies the plain language of the legislation and gives effect to each and every provision, (2) is most warranted by the legislative history and other indicia of Congressional intent, and (3) avoids a Constitutional invalidation of portions of the legislation.[9]

Accordingly, this Court holds that the SCA, either alone or in tandem with the PRS pursuant to the CALEA,[10] does not authorize access to an individual's cell-phone-derived "location information", either past or prospective, on a simple showing of articulable relevance to an ongoing investigation (a "reasonable relevance" standard).

II. STATEMENT OF CASE AND STATUTORY PROVISION AT ISSUE

Currently pending is the application of an Assistant United States Attorney re-

obtaining more information than is justified, thus requiring judicial oversight regarding minimization).

8. *Cf. United States v. United States Dist. Ct.*, 407 U.S. 297, 317, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972) (Powell, J.) ("The Fourth Amendment does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigatory and prosecutory duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks. The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy....").

9. *See, e.g., Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575, 108 S.Ct. 1392, 99 L.Ed.2d 645 (1988) (holding that " 'every reasonable construction must be resorted to in order to save a statute from unconstitutionality' "). *Cf. Warshak v. United States*, 490 F.3d 455 (6th Cir.2007), *rehearing en banc granted and opinion vacated* (Oct. 9, 2007) (concluding that SCA did not comport with Fourth Amendment, and was constitutionally invalid, to the extent disputed portions allowed disclosure of e-mail content without a warrant and without prior notice); *In re Applications of the United States for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 2007 WL 2729668 (E.D.N.Y. Sept.18, 2007) (hereafter *"Azrack E.D.N.Y. 2007 Opinion"*) (concluding that Government's reading of the PRS violated Fourth Amendment).

10. The Communications Assistance for Law Enforcement Act of 1994, 47 U.S.C. §§ 1001 *et seq.*

questing "that an Order be issued directing that (1) certain records of [a cell phone service provider] be disclosed to the Government, (2) this matter be sealed, and (3) [the cell phone service provider] and its agents be ordered not to disclose the existence of this application, order, and any disclosures pursuant thereto".

The Government has applied, under the Stored Communications Act (the "SCA"), 18 U.S.C. § 2703, for an Order requiring a cellular service provider to disclose the "transactional records"—including "historical cellular tower data", "cellular tower site information", and "sectors"—maintained with respect to a cellular telephone ("cell phone") number in the name of one individual (the "Subscriber") on the basis of its asserted relevance to an ongoing criminal investigation of another individual (the "Criminal Suspect").[11] The Government attests that the Criminal Suspect is a drug trafficker, that it is experiencing difficulty in visually surveilling that person, and that fuller knowledge of the Criminal Suspect's whereabouts is important to its counter-trafficking operations.[12] Owing to continuing technological advances, the information requested would enable the Government to identify where the Subscriber and any other individuals making use of the Subscriber's cell phone, including the Criminal Suspect, have been at any/many given times in the past and where they are likely to be now and/or in the future.

The SCA prohibits an electronic communications provider, including a cellular service provider (a "CSP"), from disclosing various stored, *i.e.* historic, subscriber telephone account information to the Government, *except on appropriate legal authority.*[13] The Government maintains that it may obtain historical cellular tower site location information (hereafter "CSLI")—and thus the location of the cell phone possessor(s)—under provisions of the SCA that authorize disclosure of "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)" under legal standards that include a Court Order issued upon "specific and articulable facts showing that there are reasonable grounds to believe that ... the records or other information sought, are relevant and

11. The Government asserts that the Subscriber's cell phone is "being used by" the Criminal Suspect. It provides no specific information connecting these two individuals, or connecting the Criminal Suspect to the cell phone. Because this Order more broadly denies the Government's request absent a showing of probable cause, it does not address the other infirmities that may arise when the Government seeks disclosure of a person's personal location information on a statement that her cell phone is being used by the target of an investigation.

12. The Government may reasonably expect that information as to the Criminal Suspect's historic whereabouts will provide valuable evidence of the locations of that person's sources of supply, "stash sites", and distribution networks. *See, e.g., 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, 135 (D.D.C.2006) (hereafter *"Facciola DDC 2006 Opinion"*) (noting Government agent's affidavit of same in requesting cellular location information). As citations to the formal captions of this genre of cases are cumbersome, we will (after the initial citation) refer to such cases by authoring Judge.

13. *See* 18 U.S.C. §§ 2702(a)(3), 2703; *see also In re the Application of the United States 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, 309 (D.P.R.2007) (hereafter *"McGiverin PR 2007 Opinion"*); Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the ECPA,* 72 Geo. Wash. L.Rev. 1557, 1568 (Aug.2004) (noting that "[t]he SCA covers retrospective surveillance") (hereafter *"Reasonable Expectations"*).

material to an ongoing criminal investigation." §§ 2703(c)(1)(B) and (d).

This Court finds that (1) the SCA expressly sets movement/location information outside its scope by defining "electronic communications" to exclude "any communication from a tracking device (as defined in § 3117)"; (2) the SCA does not establish an entitlement to information in abrogation of any other legal requirements that would otherwise apply due to the nature of that information; (3) the CALEA also expressly exempts information from a tracking device and, in legislating what information CSPs must compile/retain for disclosure to law enforcement on "Court Order or other lawful authorization", also retains the Fourth Amendment or other requirements implicated by the nature of the information sought; (4) the relevant legislative history further indicates that Congress did not intend its electronic communications legislation to be read to require disclosure of an individual's location information; to the contrary, in enacting the legislation it relied on express representations by law enforcement that it was not seeking to amend the background standards governing disclosure;[14] and (5) as reading the statutes as authorizing *ex parte* disclosure of movement/location information with no judicial review of the probable cause could violate citizens' reasonable expectations of privacy, such reading would be disfavored. This Court therefore concludes, as more fully set forth below, that it must deny the Government's requests for cellular-telephone-derived location information, historic or prospective, absent a showing of probable cause.

III. TECHNOLOGICAL DEVELOPMENT OVERVIEW

As of December, 2006, there were over 233 million cellular phone subscribers in the United States, almost ten times the number in 1994.[15] Our individual cell phones now come with us everywhere: not only on the streets, but in (a) business, financial, medical and other offices; (b) restaurants, theaters and other venues of leisure activity; (c) churches, synagogues and other places of religious affiliation; and (d) our homes and those of our family members, friends, and personal and professional associates. Indeed, many individuals no long subscribe to local wireline phones, but utilize their cell phone as their residential telephone.[16]

Cellular telephone networks divide geographic areas into many coverage areas containing towers through which the cell phones transmit and receive calls. Cell phones, whenever on, now automatically communicate with cell towers, constantly relaying their location information to the

14. *See, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F.Supp.2d 747, 764 (S.D.Tex.2005)(hereafter *"Smith SD Tex.2005 Opinion"*) (contrasting express and extensive Congressional testimony of FBI Director Freeh, in advocating for its passage, that CALEA was "intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past" and "did not relate to the SCA" with Government's subsequent assertion that it was intended to expand law enforcement's access to physical location information via the SCA).

15. *See* CTIA—The Wireless Association's Semi–Annual Wireless Industry Survey (2006), http://files.ctia.org. In 1985, when the CTIA survey was first taken, the number was 340,000. By 1994 the number of cell phone subscribers had increased to more than 24 million.

16. *See In the Matter of the CALEA,* 17 F.C.C.R. 6896, 6918 (April 11, 2002) (noting that in 1994, when the CALEA was enacted, "basic residential telephone service" was almost entirely wireline, but that households now substitute wireless telephone service).

towers that serve their network and scanning for the one that provides the strongest signal/best reception. This process, called "registration", occurs approximately every seven seconds.[17]

As we change locations, our cell phones automatically switch cell towers. Cellular telephone companies "track the identity of the cell towers serving a phone".[18] When a call is received, a mobile telephone switching office ("MTSO") gets the call and locates the user based on the nearest tower; the call is then sent to the phone via that tower. This process works in reverse when the user places a call. *See id.* In urban areas, where towers have become increasingly concentrated, tracking the location of just the nearest tower itself can place the phone within approximately 200 feet. This location range can be narrowed by "tracking which 120 degree 'face' of the tower is receiving a cell phone's signal." *Id.* The individual's location is, however, most precisely determinable by triangulating the "TDOA" or "AOA" information of the three nearest cellular towers.[19] Alternatively, the phone can be tracked extremely accurately—within as little as 50 feet—via the built-in global positioning system ("GPS") capabilities of over 90% of cell phones currently in use. *Id. See also Who Knows Where You've Been?*, 18 Harv. J.L. & Tech. at 308 (noting that, as of 2004, synchronized signal triangulation produced a 3–D location accurate to 65 feet). CSPs store cell tower registration histories and other information.[20]

In sum, as a result of the proliferation of cellular tower sites, the uniform/routine inclusion of a GPS device in cell phones, and industry's implementation of additional technology required to meet Congressional mandates, including that more precise TDOA/AOA and other location information be available to emergency-assistance providers, CSPs now compile and retain extensive personal location

17. These location signals are generally set on one band (often referred to as a "control channel"); the other frequency bands that the phone uses are for sending and receiving voice and data. *See* Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 Hastings Comm. & Ent. L.J. 421, 427 (Spring 2007) (hereafter *"Where Are We?"*); *See also Smith SD Tex. 2005 Opinion*, 396 F.Supp.2d at 750 (explaining that "control channels" are frequencies shared by the phone and base station to communicate information for setting up calls and channel changing, and that cell phone "registrations" occur "on a dedicated control channel that is clearly separate from that used for call content").

18. *In re Application of United States of American for an Order: (1) Authorizing Installation and Use of Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information, (3) Authorizing Disclosure of Location–Based Services*, 2006 WL 1876847, *1 n. 1 (N.D.Ind. July 5, 2006) (hereafter the *"Lee ND Ind.2006 Opinion"*).

19. The cell towers measure the strength of the phone's signals—and thus the phone's relative location—through a Time Difference of Arrival ("TDOA") or Angle of Arrival ("AOA") method. TDOA compares the amounts of travel time from phone to tower, while AOA measures the angles at which the phone's signals are received. The MTSO sends a signal to the cell phone's control channel when it is time to switch to the frequency of a nearer tower. *See id.*

20. Although historic call-specific registration information was at one time important for CSP billings, *e.g.*, roaming charges, with the advent of truly national networks and comprehensive cell phone "plans", it has become increasingly irrelevant to service fees, and its retention now appears related largely to cost-considerations (*i.e.*, inexpensive electronic storage of all data, without differentiation) and industry concerns that CSPs not risk under-compliance with complicated and sometimes ambiguous electronic communications regulations.

information on their subscribers and the cell phones in use.

IV. RELEVANT CONSTITUTIONAL AMENDMENT, STATUTES AND LEGISLATIVE HISTORY

A. *Fourth Amendment, U.S. Const. Amend. IV*

The Fourth Amendment establishes a fundamental protection of our right to privacy.[21] By requiring that the Government's investigation of information in which we hold a reasonable expectation of privacy be conditioned on a showing of probable cause to a detached judicial official, our understanding and implementation of the Fourth Amendment seeks to balance degrees of intrusion on our civil liberties against degrees of promotion of legitimate governmental interests.

For the reasons discussed below, this Court believes that citizens continue to hold a reasonable expectation of privacy in the information the Government seeks regarding their physical movements/locations—even now that such information is routinely produced by their cell phones—and that, therefore, the Government's investigatory search of such information *continues* to be protected by the Fourth Amendment's warrant requirement; *i.e.*, the Government must meet a probable cause background standard.[22]

B. *Wiretap and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. § 2510 et seq.*

Eighty (80) years ago, Justice Taft, writing for the majority over Justice Brandeis in dissent, concluded that a search or seizure of telephone conversations implicated no Fourth Amendment concerns because there could be no reasonable expectation of privacy in your voice projected over a wire outside of a building. *Olmstead v. United States*, 277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944 (1928). Congress responded to this interpretation with passage of the Communications Act in 1934, 47 U.S.C. § 605, which made wiretapping illegal, and which the Supreme Court confirmed to preclude wiretapping by law enforcement in *Nardone v. United States*, 302 U.S. 379, 384, 58 S.Ct. 275, 82 L.Ed. 314 (1937).

In 1967 the Supreme Court delineated the procedural safeguards imposed by the Fourth Amendment on traditional wiretapping. *Expressly because of the particular dangers of abusing electronic surveillance*, the Court required that law enforcement agents had to surmount several requirements *beyond* those of the probable cause warrant needed to search a home. *See Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); *Berger v. New York*, 388 U.S. 41, 87 S.Ct. 1873, 18

21. The Fourth Amendment's protection of privacy rights also serves the important function of protecting associational rights recognized under the First Amendment. *See Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (noting that Fourth Amendment concerns are heightened where associational interests are also at stake).

22. *See* discussion *infra* (noting that law enforcement agents have, until relatively recently, obtained Court authorization to obtain movement/location information by a showing of probable cause (or more), generally under Fed.R.Crim.P. 41 (for installation of a traditional tracking device) but sometimes under Title III (as part of a wiretapping application)). *See also Orenstein EDNY Oct. 2005 Opinion*, 396 F.Supp.2d at 322 ("I view the plain language of Rule 41 as providing a default mode of analysis that governs any matter in which the government seeks judicial authorization to engage in certain investigative activities. The Rule says as much." Concluding that "the statutes upon which the government relies to secure the requested relief do not suffice to negate the otherwise default requirement of probable cause imposed by Rule 41(d)(1)").

L.Ed.2d 1040 (1967). Congress then incorporated those procedural hurdles into the Wiretap Act passed the following year. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub.L. No. 90–351, Title III (codified as amended at 18 U.S.C. §§ 2510–2522) (hereafter "Title III").

Currently, under 18 U.S.C. § 2518, the Government may obtain a wiretap, and listen in on calls to and from a target telephone, only by demonstrating to a District Judge that (a) there is probable cause for belief that an individual has committed/is committing/will commit a specified offense; (b) there is probable cause for belief that particular communications concerning the offense will be obtained; (c) normal investigative procedures have been tried and failed or are reasonably unlikely to succeed or be too dangerous; (d) there is probable cause for belief that the facilities from which, or place where, the communications to be intercepted are/will be used, in connection with commission of the offense, are leased/listed to/commonly used by such person.[23]

With this historical background in mind, other legislation implicated by the issue *sub judice* includes:

C. *Fed.R.Crim.P. 41—Warrant Issuing Upon Probable Cause*

Rule 41 of the Federal Rules of Criminal Procedure generally provides that the Government may secure a warrant upon a showing, consistent with the requirements of the Fourth Amendment, that there is probable cause. This is the standard which the Government has long been required to meet in order to obtain Court approval for the installation and use—by law enforcement agents—of a device enabling the Government to record, or "track", the movement of a person or thing.[24]

Rule 41, as amended by the Supreme Court in 2006, expressly provides Court authority to issue a warrant for the installation and use of a tracking device (as defined in 18 U.S.C. § 3117)[25] for a renewable period not to exceed 45 days. The Rule also contains express provisions requiring notice within ten (10) days from the end of the warrant period (although it may be delayed) and the suppression of information wrongfully obtained.

As reflected in the Judicial Conference Advisory Committee's Notes to the 2006 Amendments, those amendments were in-

23. Given the additional requirements beyond ordinary search warrants, this has been referred to as both a "Title III warrant" and/or a "super warrant". *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act*, 97 NW. U.L.Rev. 607, 630 (Winter 2003).

The Courts appear to disagree as to whether the Government may request and receive CSLI when it meets the "probable cause plus" showing. *Compare, e.g., Adelman ED Wis.2006 Opinion*, 2006 WL 2871743, *4 *with Smith SD Tex.2005 Opinion*, 396 F.Supp.2d at 758.

24. *See, e.g., United States v. Karo*, 468 U.S. 705, 720, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984) (holding that use of a warrantless beeper to monitor location into private residence violates the Fourth Amendment). *Cf. also* Notes to the 1977 Amendments (noting that the trend of Supreme Court cases was to give greater priority to the use of warrants as the proper way of making a lawful search); *id.* (observing that "[i]t is a cardinal rule that ... law enforcement agents must secure and use a search warrant whenever practicable.... This rule rests upon the desirability of having magistrates rather than police officers determine when searches and seizures are permissible and what limits such be placed upon such activities.") (quoting *Trupiano v. United States*, 334 U.S. 699, 705, 68 S.Ct. 1229, 92 L.Ed. 1663 (1948), quoted with approval in *Chimel v. California*, 395 U.S. 752, 758, 89 S.Ct. 2034, 23 L.Ed.2d 685 (1969)).

25. The Committee was careful to note that it "did not intended by [the 2006] amendment to expand or contract the definition of what might constitute a tracking device." *See* Notes to the 2006 Amendment.

tended to address the use of tracking devices, "which searches [had been] recognized by statute [*i.e.*, § 3117] and by case law [*i.e.*, *United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984); *United States v. Knotts*, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983)]". The Committee further noted that the evidentiary standard applicable to the installation of a § 3117 tracking device was unspecified by "the tracking device statute" (*i.e.*, § 3117), and that the Supreme Court had "reserved ruling on the issue",[26] but that "[w]arrants may be required to monitor tracking devices when they are used to monitor persons or property in areas where there is a reasonable expectation of privacy." *See* discussion *infra* at Section V(C).

D. *Electronic Communications Privacy Act of 1986*

The ECPA, enacted in 1986, was a major overhaul of the Omnibus Crime Control and Safe Streets Act of 1968. Two of its subsections are relevant to consideration of the legal standard required for obtaining a Court Order for movement/location information:

1. *Pen Register Statute*

Historically, a "Pen Register" is a device which records or decodes electronic or other impulses which identify the *telephone numbers* dialed or otherwise transmitted on the telephone line to which such device is attached (*i.e.*, the numbers of *outgoing* calls). A trap and trace device captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electric communication was transmitted (*i.e.*, the numbers of *incoming* calls). These devices have been in long and frequent use and are collectively referred to as a "Pen Register" or "Trap and Trace".

Although they had been in use for some time, the standard applicable to the Government's installation of a Trap and Trace was not addressed until 1979, when the Supreme Court concluded that the Fourth Amendment's probable cause protections need not apply. *See Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (holding that telephone users have no reasonable expectation of privacy in the telephone numbers they dial to connect a phone call). Congress responded to *Smith* by including procedures and evidentiary standards governing the installation of a Trap and Trace in the provisions of the ECPA in 1986. *See* 18 U.S.C. § 3121 *et seq.*[27]

Although the statute requires that, absent emergency, the Government must obtain a Court Order prior to installing or using a Trap and Trace, it may do so merely upon certification "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b)(2).[28] Such Orders routinely au-

26. *Cf. In the Matter of the Application of the United States of America*, 441 F.Supp.2d 816, 836 n. 3 (S.D.Tex.2006) (hereafter "*Smith SD Tex.2006 Opinion*") ("The court has not found any case holding that a standard lower than probable cause is acceptable.").

27. The statute as enacted defined a Trap and Trace as a device for capturing "electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached." As amended by the USA PATRIOT Act of 2001, it now includes "a device or process which records or decodes dialing, routing, addressing, or signaling information." The Federal Communications Commission (the "FCC") has adopted the position, and the Court of Appeals has held, that the term "signaling information" encompasses CSLI. *See United States Telecom. Assoc. v. FCC*, 227 F.3d 450 (D.C.Cir.2000).

28. The Court's ministerial role does not include an independent review of whether the application meets the relevance standard;

thorize real-time electronic monitoring of telephone call information for a limited duration, typically sixty (60) days. *Id.* at § 3123(c).

2. *Stored Wire and Electronic Communications and Transactional Records Access*

As noted above, the SCA, a 20–year–old criminal-code statute enacted as Title II of the ECPA, *prohibits* electronic communication service providers from disclosing electronically stored, *i.e.*, historic, information to the Government, except as otherwise authorized and with appropriate legal authority.[29] More particularly, under §§ 2703(a) and (b), the disclosure of "content" information expressly requires either a Rule 41 warrant (if it has been in electronic storage with the provider for 180 days or less) or notice to the subscriber/customer together with an administrative subpoena or Court Order (if the content has been in electronic storage with the provider for more than 180 days). In contrast, the disclosure of basic account information[30] requires nothing more than an administrative, grand jury or trial subpoena. § 2703(c)(2).

The statute also provides, in § 2703(c)(1), *Records Concerning Electronic Communication Service or Remote Computing Service,* that the Government may require the release of "records or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)[31] only when the governmental entity":

> (A) obtains a warrant issued [under] the Federal Rules of Criminal Procedure,
>
> (B) obtains a court order [under § 2703(d)],
>
> (C) obtains subscriber/customer consent to disclosure,
>
> (D) submits a written request for name, address, and place of business, relevant to investigation of telemarketing fraud, or
>
> (E) seeks [basic account information] under § 2703(c)(2).

Section 2703(d), in turn, sets forth the "requirements for court order", specifying that an order for disclosure of (1) content records held by the communications provider for more than 180 days or held by a remote computing service, and to be released with notice to the subscriber/customer under subsection (b) *or* (2) "a record or other information pertaining to a subscriber to or customer of such service" under subsection (c), issue "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."

Finally, and significantly, the SCA defines "electronic communications" to expressly exclude "any communication from a tracking device (as defined in § 3117)", *i.e.*, "an electronic or mechanical device which permits the tracking of the move-

rather, it is only to review the completeness of the certification submitted. *See Lee ND Ind. 2006 Opinion,* 2006 WL 1876847 at *2.

29. *See* 18 U.S.C. § 2702(a)(3) (prohibiting, except as otherwise provided, a CSP from disclosing any "record or other information pertaining to a subscriber to or customer of such service ... to any governmental entity").

30. This information is specified to include subscriber name; address, telephone connection records/records of session times/durations; length and types of services; telephone or other subscriber number; and means/source of service payment.

31. The statute does not further define "records or other information".

ment of a person or object". *Id.* at § 2711, *Definitions* (incorporating 18 U.S.C. § 2510(12)).

E. *Mobile Tracking Device Statute, 18 U.S.C. § 3117 (1986)*

This statute, also enacted in 1986, simply provides that a Court "empowered to issue a warrant or other order for the installation of a mobile tracking device" may issue an Order authorizing its use outside the Court's jurisdiction. It broadly defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." § 3117(b). The relevant Senate Report notes that "[t]his [jurisdictional] clarification [did] not effect [*sic*] current legal standards for the issuance of such an order." S. Rep. 99-541 at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. at pp. 3555, 3588. As noted, *supra* at Section IV(C), the Government has historically been required to meet the probable cause standard for warrants set forth in Fed.R.Crim.P. 41 for Court authorization prior to installing and utilizing a tracking device.

F. *Communications Assistance for Law Enforcement Act of 1994*

(1) *Statutory Provisions*

The Communications Assistance for Law Enforcement Act of 1994 (the "CALEA"), 47 U.S.C. § 1001 *et seq.*, was intended to mandate communications carriers' acquisition and implementation of technology/equipment capable of providing law enforcement with the "wire and electronic communication" information to which it was entitled under the statutes relating to electronic communication technology. The Act required telecommunications carriers to ensure, within four (4) years from enactment (*i.e.*, by October 25,1998), that they had the ability to provide—subject to "court order or other lawful authorization"—law enforcement agencies with:

> access to call-identifying information that is reasonably available to the carrier—(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and (B) in a manner that allows it to be associated with the communication to which it pertains, except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in [§ 3127]), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number).

Id. at 1002(a)(2).

The statute defines "call-identifying information" to include "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." § 1001(2).

The CALEA, as does the SCA, expressly defines out of the "electronic communications" covered by the Act, information from a "tracking device" under § 3117. *See* § 1001(1) (adopting definitions of 18 U.S.C. § 2510).

(2) *Legislative History and Implementation*

The express purpose of the CALEA was to require communications service providers to acquire/implement technology to isolate and provide—on appropriate lawful authority—intercepted "content and call-identifying information" to law enforcement. *See* H.R.Rep. 103-827(I), *reprinted in* 1994 U.S.C.C.A.N. at pp. 3489, 3489-

90.[32] Passage and implementation of the CALEA entailed several years of extensive negotiations. The extent to which Government's investigatory access to movement/location information would be implicated/affected by a requirement that it be identified/retained/provided with appropriate authority was the subject of much testimony and debate. It was clear, however, that Congress was extremely concerned that the background requirements be preserved, and that its legislation not be later asserted to have affected the judicial review protections applicable to this constitutionally-sensitive information.

More particularly, the legislative history of the CALEA indicates that, during his lengthy and repeated testimony before the Senate and House, then-FBI-Director Louis Freeh addressed Congress' concern that with advances in cell phone technology, law enforcement could obtain—by CSLI—information of an individual's physical movement previously obtainable only through visual surveillance or the covert installation of a radio-wave transmitter. During the course of his testimony, Director Freeh reassured Congress that law enforcement was not attempting to obtain via the 1994 enactments, or to otherwise alter the standards applicable to, movement/location information. To the contrary, he asserted, the proposed legislation would "ensure[ ] the maintenance of the status quo", that it "[did] not enlarge or reduce the government's authority," and that it "*relate[d] solely to advanced technology, not legal authority or privacy*".[33]

Director Freeh's testimony included the following:

> The term "call setup information" is essentially the dialing information associated with any communication which identifies the origin and destination of a wire or electronic communication obtained through the use of a pen register or trap and trace device pursuant to court order. It does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called 'tracking' information.

Id. at 23. Director Freeh also stated, in allaying Congressional concerns:

> Law enforcement's ... ability to acquire "call setup information" ... related to dialing type information—information generated by a caller which identifies the origin, duration, and destination of a

32. *See also McGiverin PR 2007 Opinion*, 497 F.Supp.2d 301 (explaining that CALEA was passed to "*preserve* the government's ability, pursuant to court order or other lawful authorization, to intercept communications [in the face of] advanced technologies such as digital or wireless transmission modes ... while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services") (emphasis added); *United States Telecom Assoc. v. FCC*, 227 F.3d 450, 454 (D.C.Cir.2000) (citing FBI's 1994 Congressional testimony that it was "precluded ... from implementing authorized electronic surveillance" by "technological impediments" such as "the limited capacity of cellular systems to accommodate large numbers of simultaneous intercepts [and] growing use of custom calling features such as call forwarding, call waiting, and speed dialing").

33. Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings Before the Subcomm. On Technology and Law of the Senate Judiciary Comm. And the Subcomm. On Civil and Constitutional Rights of the House Judiciary Comm., 103rd Cong., 2d Sess., at 2, 28 (Statement of Dir. Freeh) (hereafter "Digital Telephony Testimony") (emphasis added); *id.* at 22 (stating that the CALEA "provide[s] law enforcement no more and no less access to information than it had in the past").

wire or electronic communication, the telephone number or similar communication address. Such information ... historically, has been acquired through use of pen register or trap and trace devices pursuant to court order.

Several privacy-based spokespersons have criticized the wording of the definition regarding this long-standing requirement, alleging that the government is seeking a new, pervasive, automated "tracking" capability. Such allegations are completely wrong.

Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from 'true' tracking devices, which can require a warrant or court order when used to track within a private location not open to public view. *See United States v. Karo*, 468 U.S. 705, 714, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984).[34] Even when such generalized location information, or any other type of 'transactional' information, is obtained from communications service providers, court orders or subpoenas are required and are obtained.

In order to make clear that the acquisition of such information is not being sought through the use of pen register or trap and trace devices, and is not included within the term 'call setup information', we are prepared to add a concluding phrase to this definition to explicitly clarify the point: *except that such information (call setup information) shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange.*

Id. at 29 (emphasis added).[35]

Finally, Director Freeh represented, in response to a letter alleging that the Government was seeking to obtain surveillance of individuals through transactional data:

> This is a false issue for a number of reasons.
>
> First, as is clearly set forth in the 'purpose' section of the proposed legislation, the intent of the legislation is to maintain existing technical capabilities and to 'clarify and define' the responsibility of common carriers ... to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information.... [It has] nothing to do with 'transactional information' under our federal electronic surveillance and privacy laws. All telecommunications 'transactional' information is already protected by federal law and is exclusively dealt with in [the SCA]. The proposed legislation does not relate to [the SCA].

Id. at 27 (quoted in *Smith SD Tex.2005 Opinion*, 396 F.Supp.2d at 763).

Following passage of the CALEA, and in accordance with Congressional direction, the Telecommunications Industry Association ("TIA") began the long process of the "development of the specific technological standards" by which industry could comply with its law-enforcement-assistance obligations. This entailed several years of negotiations and consultations amongst industry, law enforcement and consumer

34. *Cf. Facciola DDC 2006 Opinion*, 407 F.Supp.2d at 139 (explaining that a "true" tracking device was traditionally, and as in *Karo*, a radio-wave transmitter "affixed to a car that permitted its movements to be monitored").

35. *Cf. id.* at 137 (noting that "[t]he Director's offer and its acceptance by Congress led to the exception codified as 47 U.S.C. § 1002(a)(2)").

representatives "under the auspices of" the FCC. *Smith SD Tex.2006 Opinion*, 441 F.Supp.2d at 820; *see also* 47 U.S.C. § 1006.

In 1999, the FCC issued a ruling on the TIA's proposed technical specifications and protocols (which were published as the Interim Standard/Trial Use Standard J–STD–025 or the "J–Standard").[36] Six aspects of the FCC ruling were challenged and consolidated for judicial review. *See United States Telecom Assoc. v. FCC*, 227 F.3d 450 (D.C.Cir.2000). The Court of Appeals held that the agency had "acted arbitrarily and capriciously" and/or "failed to engage in reasoned decisionmaking" as to five of its interpretations of the CALEA, but that it could require CSPs to have available CSLI as "call-identifying information" under the Act. *Id.*

G. *Enhanced 911 Rules*

As individuals' use of cellular (rather than land-line) telephones rapidly expanded during the 1990s, it presented increasing difficulties for emergency service providers who had previously determined a caller's location from the account address of her stationary telephone. Beginning in 1996, and continuing over several years, the FCC issued a series of "Enhanced 911 Emergency Call Systems" rules requiring CSPs to acquire the ability to identify more precisely the locations of cell phones making emergency calls.[37]

H. *Wireless Communication and Public Safety Act of 1999*

In this legislation, amending the Telecommunications Act and authorizing a nationwide "911" emergency service for cell phone users, Congress recognized the importance of an individual's expectation of privacy in her physical location. *See* PL 106–81, 113 Stat. 1288 (Oct. 26, 1999) (amending 47 U.S.C. §§ 222, 251). More particularly, in authorizing the specifically-limited disclosure of location information to ensure the provision of emergency services, the Act directs that a customer otherwise not be deemed to have approved use/disclosure of, or access to, her CSLI absent express prior authorization. *See* 47 U.S.C. § 222(f).[38]

36. *See In the Matter of the CALEA*, 1999 WL 674884, 14 F.C.C.R. 16794 (1999). Although it modified industry's proposed technical standards in many respects, the FCC rejected some of the assistance capabilities which law enforcement sought to require. For example, the FCC rejected the New York Police Department's proposal that would have "required [CSPs to compile] triangulating signals from multiple cell antenna towers to pinpoint a wireless phone's precise location throughout a call's duration." The FCC acknowledged that providing law enforcement with triangulation capabilities would "pose difficulties that could undermine individual privacy", and concluded that "a more generalized capability that will identify only the location of a cell site, and only at the beginning and termination of the call, will give [law enforcement authorities] adequate information." *See Who Knows Where You've Been?*, 18 Harv. J. Law & Tech. at 313 (quoting 227 F.3d 450, 464 (D.C.Cir.2000)).

37. *See* 47 C.F.R. § 20.18 (2004) (requiring that licensees "achieve 95 percent penetration of location-capable handsets" among subscribers by end 2005); Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 Cardozo Arts & Ent. L.J. 381, 384–386 & nn. 23–24 (2003) (discussing CSPs' implementation of "network overlay" technology to attain the required precision).

38. *See Smith SD Tex.2005 Opinion*, 396 F.Supp.2d 747 (concluding, in discussing this legislation, 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"); *Orenstein EDNY Oct. 2005 Opinion*, 396 F.Supp.2d at 323 (similarly noting Congress' recognition of the "special nature" of location information and concluding that "a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information").

V. ANALYSIS

Any contention that the Government might obtain cell tower site location information ("CSLI") solely under the auspices of the PRS appears to have been put to bed.[39] In a series of published Orders and Opinions over the past two years, a significant majority of Courts have also rejected the Government's contention that real-time, or prospective, movement/location information may be obtained under a hybrid theory which purports to combine the authorities of the PRS and the SCA by seizing upon the term "solely" in a provision of the CALEA.[40] In so holding, many of

39. *See* CALEA; *In re Application of the United States for an Order Authorizing Pen Register and Trap and Trace Device and Release of Subscriber Information and/or Cell Site Information,* 384 F.Supp.2d 562, 563 (E.D.N.Y. 2005) (hereafter "Orenstein EDNY Aug. 2005 Order") ("The government ... appears to want to put some daylight between a pen register and the instrumentality for seeking cell site location information—notwithstanding the fact that the law plainly authorizes a court to allow the installation of a pen register on the basis of a showing that is far less demanding than the probable cause standard. Its reticence in [seeking to obtain location information through use of a Pen/Trap device] ... is understandable ... [as] Congress appears to have prohibited it from doing so.").

40. *See generally Where Are We?,* 29 Hastings Comm. & Ent. L.J. at 422–24 (summarizing that 11 of the 15 decisions published on cell phone location tracking within prior two years concluded probable cause is required, while four authorized limited prospective information).

Among the decisions denying the Government's requests for CSLI under a hybrid theory are: *In re the Applications of the United States for Orders Authorizing the Disclosure of Cell Cite Information,* 2005 WL 3658531 (D.D.C. Oct.26, 2005) (hereafter *"Robinson Joint Magistrates' DDC 2005 Order"); Facciola DDC 2006 Opinion,* 407 F.Supp.2d 134; *Lee ND Ind.2006 Opinion,* 2006 WL 1876847 (affirming Magistrate Judge's denial of application); *Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information,* 402 F.Supp.2d 597 (D.Md.2005); *In re Application of United States for Orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices,* 416 F.Supp.2d 390 (D.Md.2006); *In re Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecomm. Records,* 439 F.Supp.2d 456 (D.Md. 2006); *Orenstein EDNY Aug. 2005 Order,* 384 F.Supp.2d 562, *on reconsideration, Orenstein EDNY Oct. 2005 Opinion,* 396 F.Supp.2d 294; *In re Application of the United States for an Order for Prospective Cell Site Location Information,* 2006 WL 468300 (S.D.N.Y. Feb.28, 2006); *In re United States Application for an Order Authorizing Installation and Use of a Pen Register,* 415 F.Supp.2d 211 (W.D.N.Y. 2006) (hereafter *"Feldman WDNY 2006 Opinion"*); *McGiverin PR 2007 Opinion,* 497 F.Supp.2d 301; *Smith SD Tex 2005 Opinion,* 396 F.Supp.2d 747; *Smith SD Tex.2006 Opinion,* 441 F.Supp.2d 816, 827–37; *Adelman ED Wis.2006 Opinion,* 2006 WL 2871743, *3–4 (affirming Magistrate Judge's denial of application); *In re Application of the United States for an Order Authorizing the Disclosure of Propsective Cell Site Information,* 412 F.Supp.2d 947, 950 (E.D.Wis.2006) (hereafter *"Callahan ED Wis.2006 Opinion"*).

But see In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, 2007 WL 397129 (E.D.Cal. Feb.1, 2007) (granting request for limited prospective CSLI); *In re Application of United States for an Order,* 411 F.Supp.2d 678 (W.D.La. 2006); *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.2005) (hereafter *"Gorenstein SDNY 2005 Opinion"*); *In re Application of United States for an Order for Prospective Cell Location Information,* 460 F.Supp.2d 448 (S.D.N.Y.2006); *In re Application of the United States,* 433 F.Supp.2d 804 (S.D.Tex.2006) (hereafter *"Rosenthal SD Tex. 2006 Opinion"*); *In re Application of the United States for an Order (1) Authorizing Installation of a Pen Register and Trap and Trace Device and (2) Authorizing Release of Subscriber and Other Information,* 2007 WL 3036849 (S.D.Tex. Oct.17, 2007) (hereafter *"Rosenthal SD Tex.2007 Opinion"*) (reversing Magistrate Judge Smith's denial of application for historic and prospective CSLI).

these Courts have repeatedly opined that real-time cell-phone-derived movement/location information is "tracking" information within § 3117.[41] Few Courts have, however, addressed in published opinion whether the Government may nonetheless covertly obtain a cell phone subscriber's (or possessor's) past, or historic, movement/location information by the authority of the SCA. Some have suggested or credited (all but twice in *dicta*, and with little substantive discussion), that it may; a few have concluded or suggested that it may not.[42]

41. A District Court's published consideration of the appropriateness of *ex parte* Court Orders mandating a CSP's disclosure to the Government of an individual subscriber's location information on less than a showing of probable cause first appeared in a brief Order by Magistrate Judge Orenstein of the Eastern District of New York in late August, 2005. *See Orenstein EDNY Aug. 2005 Order*, 384 F.Supp.2d at 563 (rejecting out-of-hand the government's asserted reliance on provisions under § 2703(c) and concluding, as matter of apparent first impression, that under "only ... arguably" permissive subsection, § 2703(d), cell phone that produces CSLI revealing general geographic location is "tracking device" under § 3117 and therefore not "the *contents* of an electronic communication" obtainable under the ECPA without probable cause normally required for a warrant) (emphasis added).

Shortly thereafter, Magistrate Judge Smith of the Southern District of Texas issued a thorough Opinion providing an extensive review of the statutory history and concluding that prospective cell site data constitutes "tracking device information" under the ECPA requiring establishment of probable cause. *See Smith SD Tex.2005 Opinion*, 396 F.Supp.2d 747. At the same time, Judge Orenstein had been reviewing his earlier decision and issued a much fuller Opinion which corrected his preliminary misstep. *See Orenstein EDNY Oct. 2005 Opinion* (holding that request for prospective cell site information was effectively one for installation of tracking device, requiring at least probable cause).

Many other Courts adopted, and sometimes expanded upon, these analyses. *See, e.g., Lee ND Ind.2006 Opinion* at *4 (concluding, in affirming Magistrate Judge's denial of applications for historic and prospective CSLI, that "converging the [PRS] 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"); *Adelman ED Wis.2006 Opinion* at *5 (concluding that "[i]f the government is granted access to [CSLI], a customer's cell phone will most certainly permit tracking of his movements from place to place"); *McGiverin PR 2007 Opinion*, 497 F.Supp.2d at 310 (concluding that CSLI "does not pertain to an 'electronic communication service' within the ... SCA because it is information from a tracking device") (citing M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 Val. U.L.Rev. 1413, 1473 (2007) ("It would appear clear that on [§ 3117]'s face, a cell phone easily fits within the term 'tracking device'....")). Indeed, Magistrate Judge Smith also expanded on his own analysis the following year in *Smith SD Tex.2006 Opinion*, 441 F.Supp.2d 816.

42. *See, e.g., Callahan ED Wis.2006 Opinion*, 412 F.Supp.2d at 949 (observing, in concluding that request for prospective CSI requires probable cause—in *dicta* and without analysis—that application was "problematic" because it requested prospective rather than "historical information"); *Smith SD Tex.2005 Opinion*, 396 F.Supp.2d at 759, n. 16 (opining in *dicta* that CSPs compilation of tracking communications would bring them "more comfortably" within the scope of the SCA); *Orenstein EDNY Oct. 2005 Opinion*, 396 F.Supp.2d at 303 n. 6 (opining, in *dicta* and without explanation, that § 2703(d) "plainly allows" the Government to seek historical CSLI); *id.* at 307, n. 10 (repeating that "the SCA authorizes a[CSP]'s disclosure to law enforcement of historical cell site information, to the extent it maintains such records", this time with express citation to Magistrate Judge Smith's footnote 16); *Feldman WDNY 2006 Opinion*, 415 F.Supp.2d at 214 (accepting, in *dicta*, Government's interpretation of "the SCA [as] authoriz[ing it] to obtain *historical* [CSLI]") (emphasis in original). *See also infra* (citing *Stearns Mass.2007 Opinion* and *Rosenthal SD Tex.2007 Opinion* as only ones to expressly address and grant pending request for covert disclosure of historic CSLI by authority of § 2703).

Compare Lee ND Ind.2006 Opinion, 2006 WL 1876847 (expressly concluding, in agree-

This Court concurs with those majority opinions holding that real-time CSLI constitutes tracking information and further concludes, after extensive research and careful consideration, that a distinction between real-time ("prospective") and stored ("historic") cell-phone-derived movement/location information would be at odds with (a) the plain language and/or natural meaning of the language of § 3117 and § 2703, (b) the rule of statutory construction requiring that effect be given to each and every provision, and (c) unambiguous Congressional intent. It would also render the related provisions of the electronic communications legislation constitutionally suspect, at best. More particularly, this Court has reached the following understanding of the issues:

A. *The Government's Positions are Precluded by Textual Analysis*

1. *The Stored Wire and Electronic Communications and Transactional Records Access Statutes*

The SCA sets forth a prohibition against a CSP's release to the Government of "records or other information" pertaining to a communications service subscriber, except as otherwise authorized with, *e.g.*, warrant, consent, or court order. *See* 18 U.S.C. §§ 2702(a)(3), 2703(c), *Records Concerning Electronic Communication Service or Remote Computing Service.* In its application *sub judice,* the Government requests a § 2703(d) Order to obtain historic cellular tower site location information ("CSLI"). The Court sees two independently determinative flaws in the Government's election to predicate its request on the SCA, rather than on a probable cause warrant under Fed.R.Crim.P. 41:

(a) *An Electronic Device That Is Able and Used to Provide the Government With Movement/Location Information is a "Tracking Device", Communications From Which are (i) Expressly Excluded from the Definition of "Electronic Communications" Under the SCA and (ii) Not Pertaining to the Subscriber of an Electronic Communications Service Under the SCA*

The scope of the "Stored Wire and Electronic Communications and Transactional Records Access" Act, a subtitle of the "Electronic Communications Privacy Act", is limited to information pertaining to wire or "electronic communications", which are expressly defined to exclude communications from a device "which permits the tracking of the movement of a person or object". On its face, this definition appears to unambiguously place the information sought outside the SCA.[43]

ment with Magistrate Judge's Order, and on applications before it, that Government could acquire *neither* historic nor prospective CSLI by authority of § 2703 and absent probable cause showing under Rule 41); *Robinson Joint Magistrates' DDC 2005 Order,* 2005 WL 3658531 (directing without distinction that all applications for CSLI under either the SCA or the PRS, or both, be returned to the government). *Cf. McGiverin PR 2007 Opinion,* 497 F.Supp.2d at 303 (characterizing prospective nature of request for cell site information as "[i]mportant" without elucidation); *but see id.* at 310 ("The SCA's trail of definitions leads, inescapably in my judgment, to the conclusion that the discloseable information under the statute does not include location information."). *Cf. also In re Applications of the United. States for Orders Pursuant to § 2703(d) to Disclose Subscriber Information and Historic Cell Site Information,* 509 F.Supp.2d 64, 66 (D.Mass.2007) (Alexander, M.J.) (hereafter *"Alexander Mass.2007 Opinion"*) (holding that disclosure of historic CSLI is subject to probable cause standard of Rule 41), *rev'd,* 509 F.Supp.2d 76 (D.Mass. 2007) (hereafter *"Stearns Mass.2007 Opinion"*).

43. *Cf. Steve Jackson Games, Inc. v. United States Secret Service,* 36 F.3d 457, 461 (5th Cir.1994) ("Understanding the [ECPA] requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analy-

As technology now stands (and it will no doubt continue to rapidly evolve), triangulation of CSLI enables a covert observer to know our physical movements/locations within 50 feet; and our cell phones, whenever on, broadcast this information virtually continuously as we go about from place to place. Even without triangulation, our cell phones transmit—and our CSPs record—information of our movements to a few hundred feet. It is, therefore, extremely difficult to see how a cell phone is not now *precisely* an "electronic ... device which permits the tracking of the movement of a person or object." § 3117(b).[44]

By virtue of cell phone technology, law enforcement may now electronically monitor our movements with as much—indeed, ofttimes more—scope and precision as by its traditional methods of visual surveillance and/or installation of a "beeper". As other Courts have observed, tracking device and cell phone technologies have *converged.* That is, our cell phones—when utilized to record our physical movements—operate in the same manner and to the same purpose as earlier radio-wave beepers.[45] This Court concurs, therefore, with the several thorough and thoughtful opinions to have reviewed the statutory language and reached this same conclusion.

With those Courts that have opined (or assumed) that the Government may none-

sis.") (quoted with approval in *Smith SD Tex. 2005 Opinion,* 396 F.Supp.2d at 753 (concluding that "rigorous attention must be paid to statutory definitions")).

44. The Court notes, moreover, as others have pointedly and repeatedly observed, that the sweeping definition of § 3117 does not rely on a particular degree of precision. *See, e.g., Smith SD Tex.2005 Opinion,* 396 F.Supp.2d at 753 (rejecting as "unpersuasive" argument that CSLI is not "information from a tracking device" because it does not provide "detailed" location information); *Smith SD Tex. 2006 Opinion,* 441 F.Supp.2d at 836–37 (concluding that limitations placed on subsequent request for CSLI did not alter prior conclusions); *id.* at 828 n. 28 (collecting cases rejecting narrowed requests); *McGiverin PR 2007 Opinion,* 497 F.Supp.2d at 310 (noting courts' acknowledgment that § 3117 is "striking in its breadth"); *Feldman WDNY 2006 Opinion,* 415 F.Supp.2d at 219 ("There is nothing in the legislative history of the CALEA to suggest that the exception clause [for location information] was intended by Congress to create some sort of sliding scale ..., with the evidentiary standard for disclosure hinging on the type or duration of ... signaling information sought."); *Orenstein EDNY Oct. 2005 Opinion,* 396 F.Supp.2d at 310–11 (concluding that application for limited CSLI did not affect applicability of § 3117, which "does not distinguish between general vicinity tracking and detailed location tracking"); *Callahan ED Wis.2006 Opinion,* 412 F.Supp.2d at 957 ("[E]ven such less precise location information was included in the 'tracking information' about which Congress was concerned"); *Adelman ED Wis.2006 Opinion,* 2006 WL 2871743 at *3 n. 2 (affirming Magistrate Judge's denial despite limitation of CSLI sought to J–Standard information).

Cf. Smith SD Tex.2006, 441 F.Supp.2d at 828, n. 27 (noting that "[one law enforcement agent had] candidly conceded that [the] strategy [of requesting more limited CSLI] is guided not so much by legal principle as by a desire to placate recalcitrant magistrate judges") (citing *Feldman WDNY 2006 Opinion*).

45. *See, e.g., Smith SD Tex.2005 Opinion,* 396 F.Supp.2d at 751 (summarizing that "a cell phone is (among other things) a radio transmitter that automatically announces its presence ... via a radio signal over a control channel" and by which "law enforcement is able to track the movements of the target phone"); *id.* at 754 (recounting law enforcement's "pinging" (calling without allowing to ring) suspect's cell phone and using location information to re-establish visual surveillance); *id.* at 755 (noting as only difference that cell phone is on person instead of attached to vehicle); *id.* (observing that by adopting broad language "Congress may simply have been anticipating future advances in tracking technology [which have] indeed come to pass").

theless acquire historic cell-phone-derived movement/location information by a § 2703(d) Order, we must, however, respectfully disagree. The Court finds two possible explanations for this largely-unexplained distinction between prospective and historic CSLI: (i) that stored CSLI is somehow no longer information from a tracking device excluded by § 3117 (or perhaps that, unlike real-time CSLI, it should not be regarded as such because its disclosure is somehow less intrusive or otherwise less entitled to protection); or (ii) that stored CSLI remains outside the Act's definition of an "electronic communication" but is nonetheless within the scope of § 2703(c) because it is information that pertains to a subscriber of an electronic communication (*i.e.*, cell phone) service.

(i) Historic CSLI Properly Remains Information from a Tracking Device, Excluded from the Definition of an "Electronic Communication"

The first explanation is tantamount to an assertion that the *mere storage* of what appears indisputably to be information from a tracking device when garnered, alters its character. No such archival alchemy is possible. The frequent and specific information of our physical movements now transmitted by our cell phones is, necessarily, *and remains,* information from a device that permits the tracking of movement. The source of information does not change when it is stored. Communication from a "tracking device", whether released to law enforcement instantaneously or with some interval of delay, is communication from a "tracking device".[46]

Not only would acceptance of a contention that stored, or past, movement/location information is no longer "communication from a tracking device" fail to correspond to normal usage,[47] it would render the SCA's express exclusion of such information superfluous. More particularly, the SCA's scope is expressly limited to "stored" communications, *i.e. only* past data,[48] and yet it also defines the stored electronic communications within its scope to exclude communications from a tracking device. An interpretation of "information from a tracking device" as *not* encompassing such information once stored would effectively *read out* this express limitation on what may constitute an "electronic communication" for purposes of the Act.[49]

46. Some of the language of Magistrate Judge Smith's 2005 decision suggests that he attached significance to the real-time nature of the CSLI being sought in that case. *See, e.g., Smith SD Tex.2005 Opinion,* 396 F.Supp.2d at 759. As discussed *infra,* this Court believes that this interpretation fails to give appropriate scope to the language of the statutory exception.

47. In the normal contemplation of the language, evidence of past movement is precisely "tracking" information. Location is static; movement is change in location. There is, thus, a temporal element inherent in the term "movement"; one can *only* "track" location over time. *See Smith SD Tex.2005 Opinion,* 396 F.Supp.2d at 756 (explaining that CSLI "allows continuous tracking of actual movement, *i.e.,* change of location over time"). There is no reason to believe that this does not include *past* time. To the contrary, one can *only* "track" movement (*i.e.,* changes in location) that has happened *in the past.* Indeed, the apparent origin of the term "track" derives from looking at the physical manifestations of the prior presence of the subject being tracked to reconstruct or trace a course of movement. Conceptually, then, tracking means looking at evidence of past presence, *i.e.,* it is necessarily backward-looking.

48. *See, e.g., McGiverin PR 2007 Opinion,* 497 F.Supp.2d at 309 (noting that SCA contemplates orders for stored information and therefore lacks provisions typical of prospective surveillance statutes, such as time limits, provisions for renewal, or automatic sealing of records).

49. *See Cooper Inds., Inc. v. Aviall Servs., Inc.,* 543 U.S. 157, 158, 125 S.Ct. 577, 160 L.Ed.2d 548 (2004) (repeating settled rule that Court

(ii) Information Expressly Excluded from the ECPA (including the SCA) as Outside the Scope of the Term "Electronic Communication" Cannot Reasonably Be Re-Included as "Pertaining to" a Subscriber or Her Electronic Communication Service

CSLI, as communication from an electronic device that permits the tracking of an individual's movements/locations, is information of a nature expressly set aside by definition. To then say that stored information from a tracking device nonetheless comes directly back—as a record pertaining to an electronic communication service—[50] into the scope of the SCA, a statute that carefully exempts tracking-device communications from its definition of "electronic communication", would abrogate that express limitation. As the principal subject of this legislation was to describe the information encompassed and delineate certain procedures regarding its disclosure to law enforcement, there could be no possible purpose to the "tracking device" exclusion other than to limit the disclosure of stored information derived such devices.

This Court sees, therefore, no way to reconcile the express exclusion of tracking device information with the remainder of the statutory language but to read the provision of § 2703(c) to authorize disclosure of records and other information *directly* pertaining to a subscriber/customer of an electronic communication service. That is, information that is regarding or derived under a service (*e.g.*, a tracking capability/function) that may be used to facilitate the provision of an electronic communication service (*e.g.*, the transmission of voice/text material),[51] but that is not *itself* an electronic communication service (as, *e.g.*, by definition), does not "pertain" to the subscriber of an electronic communications service within the meaning of the statute.[52]

must, if possible, "construe statute to give every word operative effect").

Because the SCA carefully sets apart tracking device information from its legislation of stored information, it appears to acknowledge that the passage of time does not alter the constitutionally-sensitive character of such information. *Cf. Alexander Mass.2007 Opinion, rev'd Stearns Mass.2007 Opinion,* 509 F.Supp.2d at 74 ("[T]he same Fourth Amendment concerns that drive the necessity for a probable cause showing before authorization of a prospective tracking device apply equally to a 'historical' tracking device."); *id.* (observing that the "central inquiry" turns on the reasonable expectation of privacy under *Katz*).

50. The SCA's coverage of records or other information under § 2703(c)—if not otherwise excluded—turns on whether the information "pertains to" the subscriber of a covered communications service *in her capacity as such.* This interpretation is consistent with the heading of § 2703(c) and Magistrate Judge Smith's conclusion that, based upon the legislative history, "[t]he records to be disclosed must pertain to the subscriber's *use* of the provider's electronic communication service". *Smith SD Tex.2005 Opinion,* 396 F.Supp.2d at 758 (emphasis added) (quoting S.Rep. No. 99-541 at 38, 1986 U.S.C.C.A.N. at pp. 3555, 3592).

51. *See* 18 U.S.C. § 2510(15) (defining an electronic communications service as one that "provides to users thereof the ability to send or receive wire or electronic communications").

52. Magistrate Judge McGiverin of the District Court for the District of Puerto Rico has recently taken a similar path to a similar conclusion, to wit: Because CSLI derived from the control channel transmissions of a cell phone permits determination of the phone's location over time (i.e., tracking of its movement), the acquisition/collection of such information uses the cell phone (or its control channel subsystem) as a tracking device. Thus these (separate/separable) control channel communications do not constitute "electronic communications", and the systems for transmitting and receiving them do not constitute electronic communications service. *See McGiverin PR 2007 Opinion,* 497 F.Supp.2d at 310-11 (agreeing with cited au-

To put this another way: Although some Courts have opined or suggested (again, almost always in *dicta*) that the registration, or subsequent storage, of CSLI pertains to a subscriber's electronic communications service because it is used to facilitate the provision of that service, or because the CSPs compile it,[53] this

thorities that "when a cell phone is used to determine a person's location it falls within the meaning of a tracking device under the plain language of" § 3117, thus "cell site information cannot constitute an 'electronic communication'" and such information therefore "does not pertain to an 'electronic communication service' within the meaning of the SCA"); *id.* at 310 (concluding that "the SCA's trail of definitions leads, inescapably in my judgment, to the conclusion that the discloseable information under the statute does not include location information").

Also similarly, Magistrate Judge Smith has syllogized that

> a communication from a tracking device, such as [CSLI], is neither an electronic nor a wire communication under the ECPA, and so it does not fall within the range of covered services provided by an 'electronic service provider'. And since a subscriber does not use the phone to track his own movements in real time, prospective [CSLI] appears to be unrelated to any *customer* (as opposed to law enforcement) use of the provider's services. Thus, painstaking and methodical analysis of the SCA's technical terms offers no support for treating prospective [CSLI] as a transactional record under § 2703(c)(1).

Smith SD Tex.2005 Opinion, 396 F.Supp.2d at 759. Magistrate Judge Smith went on to opine in a footnote, rather surprisingly, that "[b]y contrast, historical [CSLI] more comfortably fits within the category of transactional records ... [because CSPs] might legitimately compile such data for customized marketing and billing purposes." *Id.* at n. 16. It is unclear to this Court how compilation for the provider's purposes would bring otherwise excluded tracking communications within the *customer's use* standard so carefully delineated in Magistrate Judge Smith's thoughtful opinion. The Court also notes that, more recently, Magistrate Judge Smith—in granting portions of the Government's applications for various electronic communications information under the PRS and SCA—denied requests for historic and prospective CSLI. *Cf. Rosenthal SD Tex 2007 Opinion*, 2007 WL 3036849, *1 (reversing as to both).

53. *See Smith SD Tex.2005 Opinion, supra* n. 54. *See also Stearns Mass 2007 Opinion*, 509 F.Supp.2d 76 (concluding that historical cell site information is a record or other information pertaining to a customer, as it contains data specific to the handling of a customer's call). This succinct Opinion is, to this Court's knowledge, one of only two published Opinions to hold, in deciding a presented question, that covert disclosure of historic CSLI *may* be made to the Government under § 2703 on a showing of less than probable cause. *Id.* at 79, n. 5 ("Although no published opinion has directly addressed the issue, a number of courts have assumed or implied in *dicta* that the disclosure of historical date is proper under the SCA's specific and articulable facts standard."). *But see Lee ND Ind.2006 Opinion*, 2006 WL 1876847 at *1 (expressly concluding, in affirming Magistrate Judge, that Government's separate applications for historic and prospective CSLI each requested information "unobtainable absent a warrant").

In reversing Magistrate Judge Alexander's denial of the Government's applications for the release of historic CSLI under the SCA, Judge Stearns did not analyze whether a cell phone constitutes a tracking device when used to transmit location information, or whether such information pertains to a service covered under the SCA. Instead, he apparently considered this statutory analysis to be a mere "analogy", with which he disagreed because:

(1) He concluded that excluding CSLI from the "records and other information" obtainable under 2703(d) would leave nothing subject to that subsection's intermediate standard, as all other non-content information might be obtained under the less stringent requirements for a subpoena under 2703(c)(2). *See* 509 F.Supp.2d at 80 n. 8. This disregards that call-identifying information—*i.e.*, the incoming and outgoing phone numbers traditionally obtained through a Trap and Trace—constitutes information pertaining to a cell phone subscriber that is *not* obtainable by subpoena under § 2703(c)(2); and

(2) He observed that "nothing in the 18 U.S.C. § 3117(b) definition of a mobile tracking device places a limitation on the 'records

Court must strongly disagree. To the contrary, and even if a reading of § 2703(c) as re-including CSLI did not raise application-based concerns,[54] it is

or other information' obtainable pursuant to a section 2703(d) order." *Id.* This observation merely begs the question. If § 2703(c) limits disclosure to information pertaining to a service covered under the SCA (*e.g.*, electronic communication), and the Act's definitions place communications from a tracking device as defined in § 3117 outside the scope of "electronic communications", then the limitation against disclosure of tracking information follows (as set forth above) despite the absence of a reference to § 2703 in the text of § 3117. (Judge Stearns also noted that he was unpersuaded "of the relevance of" § 3117 to the issue, since that statute "governs the 'installation of tracking devices'." *Id.* at 81 n. 11. This overlooks the SCA's express definitional incorporation of § 3117.)

Finally, Judge Stearns held that disclosure of historic CSLI would implicate no Fourth Amendment concerns because:

(1) "historic information that ... reveal[s] where a subject of interest [was] in the past ... will not ... tell the government anything about the subject's [present or future locations]." *Id.* at 81. To the contrary, where we have been provides a *great deal of information* not only as to our previous movements/locations but as to our on-going activities and associations, *i.e.*, our current and prospective movements/locations. Indeed, the Government requests it for these reasons. Moreover, the privacy and associational interests implicated are the same. Some degree of delay in the secretive disclosure to law enforcement does not diminish—certainly not meaningfully—the degree of intrusion/infringement on our civil rights.

(2)"even if an order requiring the disclosure of prospective cell site information allowed the government to 'track' a suspect ... into a protected area like a home" no "reasonable Fourth Amendment expectation of privacy [would] be compromised" because "the most [it] might reveal is that [the possessor] might be found in the home" and "[t]here is nothing ... about that disclosure that is any more incriminating or revealing than what could be gleaned from activation of a pen register or from physical surveillance." *Compare* CALEA (expressly prohibiting disclosure of location information via Trap and Trace); *Karo*, 468 U.S. at 716, 104 S.Ct. 3296 (rejecting "Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether ... a person ... is in an individual's home at a particular time"); *infra* at Section V(C) (addressing Fourth Amendment considerations). *Cf. Warshak, supra*, (noting that our privacy interests go beyond not wanting to be incriminated).

See also Rosenthal SD Tex.2007 Opinion, 2007 WL 3036849 (concluding, with citation to Judge Stearns, that the Government could require covert disclosure by the CSP of *both* historic and prospective CSLI by application under the SCA and under a hybrid theory, respectively). In this Opinion, the only other published Opinion to order disclosure of historic CSLI under the § 2703(d) standard, Judge Rosenthal recently reversed Magistrate Judge Smith's denial of applications for historic and prospective CSLI, holding that (i) both were "records" within § 2703(c)(1); and that (ii) essentially real-time information could be produced under the hybrid theory so long as it was communicated through the CSP and not directly to the Government. *Id.* at *4–6. This Opinion, which was contrary to the weight of authority in several respects, acknowledged, but did not analytically refute, other Court's "tracking device" concerns, except to suggest that its approval of applications for *limited* CSLI "minimiz[ed] the concern that a cell phone could be used as a kind of 'tracking device'." *Id.* at *3–5. *See also Rosenthal SD Tex.2007 Opinion* at *6 (noting, in closing, that any speculation about improper use would be premature). *Compare Where Are We?*, Hastings Comm. & Ent. L.J. at 433, n. 65 (noting that, "without judicial oversight, it becomes rather difficult to ascertain whether the reality of [electronic communications] surveillance suggests abuse").

54. If § 2703(c) were read to require, with appropriate legal authority, the disclosure of communication from a tracking device "pertaining" to a covered service, the inclusion of records of cell-phone-derived movement/location information would remain far from clear. The subscriber, for her part, is expending her monthly funds for the electronic communication of content (*e.g.*, voice or text), not to

necessary—for reasons of statutory and Constitutional interpretation—to read § 2703(c)'s authorization for disclosure of records or information pertaining to a subscriber of an electronic communication service to exclude any movement/location information derived from her cell phone, even if incident thereto. If the excluded tracking information were brought back in, Congress' exclusion of tracking device communications from the definition of "electronic communication" would be a pointless gesture, with no actual effect. It is apparent to this Court that Congress intended by the exclusion of tracking devices in the statutory definition that the SCA not become a vehicle for diminishing the long-recognized protections against covert disclosure of movement/location information; and it behooves the Court to interpret the SCA in a manner that gives effect to that intent.

For these reasons, this Court concludes that CSLI is communication from an electronic device that permits the tracking of the movement of a person, is therefore expressly placed outside the scope of the electronic communications legislation of the SCA, and is not appropriately brought back into the scope of information which the Government may seek to obtain thereunder by any reasonable reading of § 2703(c).[55]

record her physical/geographic movements. The CSP, for its part, utilizes some portion of the automatically-registered CSLI to complete the subscriber's calls. Much of that seven-second information, however, becomes irrelevant; and the historic record showing her changes in location over time does *not* pertain, even indirectly, to her cell phone service. Questions might also remain regarding the extent to which even specific-call-facilitating CSLI is stored information pertaining to the subscriber's cell phone service when retention of that information is now principally—if not exclusively—to ensure the CSP's compliance with legislative mandates.

(b) ***Even if Cell–Phone–Derived Location Information Were Within Its Scope, The SCA Neither Establishes An Entitlement to Movement/Location Information Under a Reasonable Relevance Standard Nor Otherwise Abrogates Otherwise Applicable Standards***

Even if the movement/location information now derivable from our cell phones, *i.e.*, CSLI, were interpreted to be something other than information communicated from an electronic device "which permits the tracking of the movement of a person", and/or even if it were interpreted to be re-included in the scope of the SCA as information pertaining to a subscriber or her use of an electronic communication service, it *remains* information of a character which has traditionally required a showing of probable cause/warrant under Fed.R.Crim.P. 41. And *neither* of the provisions on which the Government has relied in asserting entitlement to such information under a "reasonable relevance" standard suggests any Congressional alteration of that background rule. More particularly:

(i) Section 2703(c) provides that the Government may require that the CSP disclose subscriber information (other than content) "only when", after which follows a line-item list of alternative standards un-

55. The Court emphasizes that the foregoing analysis rejects a distinction between historic and prospective CSLI for purposes of § 2703(c). This Court believes that its analysis is consistent with the fine statutory analyses of Magistrate Judge McGiverin, of Magistrate Judge Smith's pioneering and highly-influential opinion, and of Magistrate Judge Orenstein and others, whose holdings ultimately also did not depend on any such distinction. It observes that Judge Lee has reached the same express conclusion as to the requirement of a probable cause warrant for a CSP's disclosure to Government of historic or prospective CSLI.

der which such subscriber information may be legally obtained, *i.e.:* by warrant; court order under § 2703(d); subscriber consent; or, for telemarketing fraud or basic account information, another; *de minimis*, standard. Although it specifically links these last two categories of information to compliance with a specific standard, as to the remaining category of unspecified "records and other information" it simply recites those standards potentially applicable to non-content information, including a warrant issued under the Federal Rules of Criminal Procedure. Congress' recitation of potentially-applicable standards, without more, cannot be read to replace the probable cause warrant requirement otherwise applicable to these tracking device communications with an entitlement to that same information under a reasonable relevance standard.

(ii) Similarly, nothing in the language of § 2703(d) indicates that information requested by the Government is obtainable as a matter of course upon a showing of reasonable relevance to a criminal investigation. To the contrary, § 2703(d) provides that an Order for disclosure shall issue "only if" the Government shows that the information sought is relevant. It does not provide that such an Order shall issue "if" or "whenever" such a showing is made. Thus, under the plain language of the SCA, a showing of reasonable relevance is a *necessary*, but not necessarily *sufficient*, condition for issuance of an Order. This statutory provision is linguistically and logically equivalent to a directive that an Order shall not issue if the Government does not make the required showing of relevance; the statute is simply silent on what other requirements might apply where the Government shows reasonable relevance.[56]

The Government has argued, and some Courts have uncritically assumed, that it is entitled to a § 2703(d) Order whenever it makes the required relevance showing (as if the SCA read "if" or "if and only if" rather than "only if"). In addition to being contrary to the plain meaning of the language used in the statute, the Government's interpretation would dramatically, and probably unconstitutionally, decrease the protections afforded not only to subscribers' location information, but also to the content of stored communications such as emails and voice mails. More particularly, if issuance of a § 2703(d) Order were mandatory whenever the government made the showing contemplated therein with respect to records or other information under § 2703(c), then the same statutory language would mandate issuance of an Order for disclosure of content (stored more than 180 days) under § 2703(b) upon the same minimal showing. Such a mandatory outcome would render the SCA's further requirement of prior notice (under § 2703(b)(1)(B)), in those instances in which the Government did not invoke the delay provisions of § 2705,[57] a

56. *See, e.g., Miller-El v. Cockrell*, 537 U.S. 322, 349, 123 S.Ct. 1029, 154 L.Ed.2d 931 (2003) (where statute provides for issuance of a certificate of appealability "only if" the applicant has made a substantial showing, such showing "*does not entitle* an applicant to a COA; it is a necessary and not a sufficient condition") (emphasis in original); *California v. Hodari D.*, 499 U.S. 621, 628, 111 S.Ct. 1547, 113 L.Ed.2d 690 (1991) (concluding, regarding *Menderhall* test, *i.e.*, that a person has been seized within the meaning of the Fourth Amendment "only if ... a reasonable person would have believed he was not free to leave": "It says that a person has been seized 'only if', not that he has been seized 'whenever'; it states a necessary, but not a sufficient, condition.").

57. The Government may request delayed notice on showing that prior notice would, *e.g.*, endanger life/physical safety, risk criminal flight, evidence destruction, or witness intimidation.

hollow protection of the subscriber's privacy interest in the content of stored email and voice mail.[58] The Court concludes, therefore, that the issuance of an Order under § 2703(d) remains circumscribed by otherwise applicable legal requirements according to the nature of the records or information sought. In the case of movement/location information derived from an electronic device, the traditionally-applied legal standard has been a showing of probable cause; and nothing in the text, structure, purpose or legislative history of the SCA dictates a departure from that background standard as to either historic or prospective CSLI.[59]

2. *The Communications Assistance for Law Enforcement Act of 1994*

As noted above, a significant majority of Courts have rejected the Government's contention that real-time, or prospective, movement/location information may be obtained under a hybrid theory which purports to combine the authorities of the PRS and the SCA by seizing upon the term "solely" in a provision of the CALEA. This Court need not tarry on this widely—and rightly—refuted contention, particularly as the United States Attorney for this District is no longer pursuing this position. *See supra* n. 4.[60]

58. *Cf. Warshak v. United States*, 490 F.3d 455, 473 (6th Cir.2007), *vacated and rehearing en banc granted* (Oct. 9, 2007) (recognizing privacy interest in content of stored emails and calling related provisions of SCA into Constitutional question); *id.* at 469–76 (holding that where there is a reasonable expectation of privacy, probable cause standard controls, including particularity requirement).

59. *See Lee ND Ind.2006 Opinion*, 2006 WL 1876847 (affirming denial of Government's applications for historic and prospective CSLI); *id.* at *1 (concluding that *"[e]ither way* ... an order requiring cellular phone companies to identify the specific cell tower from which a call originates, is maintained, or received" is "unobtainable absent a warrant"). *Cf. Robinson DDC 2005 Order*, 2005 WL 3658531 (denying Government's applications for Orders authorizing the disclosure of cell site information by authority under either § 2703, §§ 3122 and 3123, or both); *id.* (noting that "neither [SCA nor PRS] expressly authorizes the disclosure of cell site information" and concluding, with no distinction as to historical or prospective CSLI, that "[a]bsent new authority which dictates a different exercise of discretion", Magistrates will not grant applications absent a showing of probable cause). *Cf. In re CALEA*, 227 F.3d 450 (D.C.Cir.2000) (noting that "all of CALEA's required capabilities are expressly premised on the condition that any information will be obtained 'pursuant to a court order or other lawful authorization' " and thus CALEA does not authorize modification of either "evidentiary standards or procedural safeguards").

60. *See Orenstein EDNY Aug. 2005 Order*, 384 F.Supp.2d at 565 ("[W]here a carrier's assistance to law enforcement is ordered on the basis of something less than probable cause, such assistance must not include disclosure of ... physical location"); *Feldman WDNY 2006 Opinion*, 415 F.Supp.2d at 219 (accepting government's testimony that CSLI providing more than *general* location information would be governed by a *probable cause* standard, Congress would have "recognized the same concern and intended that the [PRS] be paired with Rule 41"). *Cf. Alexander Mass. 2007 Opinion, rev'd, Stearns Mass.2007 Opinion*, 509 F.Supp.2d at 72 ("Through CALEA, Congress [intended] to close a loophole that would have allowed government agents" to obtain location information "without a showing of probable cause").

The Court also notes that the CALEA expressly exempts communications from a tracking device (defined in § 3117) from its definition of "electronic communications" and, in legislating what information CSPs must compile/retain for disclosure to law enforcement on "Court Order or other lawful authorization", also retains the Fourth Amendment or other requirements implicated by the nature of the information. *See* analysis of similar aspects of the SCA, *supra*.

B. *The Government's Positions are Contrary to Legislative History*

The foregoing textual analysis is strongly bolstered by a clear and consistent thread in the legislative history of various electronic communications statutes reflecting Congress' continuing recognition of a privacy right in certain electronic communications information, including location information, and a corresponding intent to safeguard such information against disclosure under standards that would erode traditional Fourth Amendment protections.[61]

As discussed extensively above, the relevant legislative history indicates that Congress did not intend its electronic communications legislation to be read to require, on its authority, disclosure of an individual's location information; to the contrary in enacting the legislation it relied on express representations by law enforcement that it was not seeking to amend the background standards governing the disclosure of movement/location information.[62] The ECPA and the CALEA were careful to exempt communications from an electronic device capable of tracking our movements from their definitions of "electronic communications"; the history of the CALEA is replete with expressions of concern that it not be understood to alter the evidentiary standards (and testimony allaying those concerns); and the Wireless Communication and Public Safety Act expressly recognized the importance of an individual's expectation of privacy in her physical location. Accordingly, the legislative history has contributed to and reaffirmed this Court's understanding of the Congressional intent reflected in the statutory text.

C. *The Government's Positions Would Render the Statutory Schemes Constitutionally Suspect*

This Court concludes, as a matter of statutory interpretation, that nothing in the provisions of the electronic communications legislation authorizes it to order a CSP's covert disclosure of CSLI absent a showing of probable cause under Rule 41. And this interpretation is abundantly confirmed by consideration of the Constitutional principles at issue. For reading the statutes in the manner advocated by the Government would, as to at least a substantial portion of the information at issue, violate Americans' reasonable expectation of privacy in any cell-phone-derived information/records as to their physical move-

61. *Cf. Smith SD Tex.2006 Opinion,* 441 F.Supp.2d at 826 (summarizing legislative history "reflect[ing] persistent Congressional efforts to assure that communications content retain their protected legal status in the face of changing technology and law enforcement capabilities"); *Reasonable Expectations,* 72 Geo. Wash. L.Rev. at 1559 (providing extensive history to ECPA, enacted at time of "growing consensus [including] among members of Congress ... that advances in telecommunications, such as wireless telephones and e-mail, were outpacing existing privacy protections ...."); *id.* at 1563–1565 (discussing Electronic Surveillance and Civil Liberties Report, prepared by the Office of Technology Assessment at Congress' behest in 1985).

62. *See supra* at Section IV. *Cf. Smith SD Tex.2005 Opinion,* 396 F.Supp.2d at 751–52 ("The ECPA was not intended to affect the legal standards for the issuance of orders authorizing [tracking] devices.") (citing H.R. Rep. 99–647 at 60 (1986)); H.R. Rep. 103–827 at 17, *reprinted* at 1994 U.S.C.C.A.N. 3489, 3497 (Oct. 4, 1994) (noting that "as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited" and that CALEA "add[ed] protections to the exercise of the government's current surveillance authority"); *Orenstein EDNY Oct. 2005 Opinion,* 396 F.Supp.2d at 306 (noting that "the House Judiciary Committee sought quite emphatically to quell concerns about how the proposed legislation might infringe Americans' privacy rights").

ments/locations by authorizing *ex parte* disclosure of that information with no judicial review of the probable cause. It appears to this Court, from its review of current Fourth Amendment case law and Constitutional principles, that this information is entitled to the judicial-review protections afforded by a probable cause warrant and historically applied to movement/location information derived from a tracking device.[63] And its understanding informs the Court's interpretation of the statute, just as it believes Congressional understanding of the same principles motivated statutory limitations.

Even if the Government's proffered interpretation did not impermissibly strain both the statutory language and legislative history, the doctrine of Constitutional avoidance counsels the choice of a limiting interpretation that does not require the Courts repeatedly, on an *ex parte ad hoc* basis, to delineate the precise bounds of Fourth Amendment protection.[64]

As discussed earlier, the Fourth Amendment prohibits unreasonable searches and seizures and, accordingly, the Government must generally demonstrate probable cause and obtain a warrant prior thereto. To trigger the Fourth Amendment's protections, the individual must have a subjective expectation of privacy in the object of the Government's search, and it must be one which society accepts as objectively reasonable.[65]

The Court believes, based on common experience within the community:[66] First, that Americans do not generally know that a record of their whereabouts is being created whenever they travel about with their cell phones, or that such record is likely maintained by their cell phone providers and is potentially subject to review by interested Government officials.[67] And second, that most Americans would be appalled by the notion that the Government could obtain such a record without at least a neutral, judicial determination of probable cause.[68]

63. Indeed, some Courts have suggested that in light of the heightened vulnerability of electronic surveillance to abuse for reasons of, *e.g.*, cost and undetectability, together with the heightened concerns following from its breadth and potential over-inclusiveness, CSLI should be afforded additional judicial safeguards, such as those provided under 18 U.S.C. § 2158. *Cf. Orenstein EDNY Oct. 2005 Opinion,* 396 F.Supp.2d at 322 (noting that opinion did not "decide that a showing of probable cause necessarily suffices to permit the installation of ... a [Trap and Trace] and using it to acquire the [CSLI] transmitted over a control channel" and that it may be "that there is in fact a *more* exact showing that the government must make").

64. *See Ashwander v. Tennessee Valley Authority,* 297 U.S. 288, 348, 56 S.Ct. 466, 80 L.Ed. 688 (1936) (Brandeis, J., concurring) ("When the validity of an act of the Congress is drawn in question, and even if a serious doubt of Constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided."). *Cf. Smith SD Tex.2006 Opinion,* 441 F.Supp.2d at 837 ("Given the presence of a competing interpretation which is not only plausible but more consistent with the statutory text and legislative history, [the] canon of [constitutional avoidance] weighs decisively against the Government's position.").

65. *See Katz,* 389 U.S. 347, 88 S.Ct. 507; *California v. Greenwood,* 486 U.S. 35, 39, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988).

66. The Magistrate's role as arbiter of reasonableness in a search warrant application inherently acknowledges, and is predicated upon, her representation of community sensibilities.

67. *See Who Knows Where You've Been,* 18 Harv. J. Law & Tech. at 313 (observing that "few customers are likely to appreciate the specificity of the location information available to service providers and the fact that companies can retain it indefinitely").

68. *See* Brief of the Federal Defenders of New York as *Amicus Curiae* in *Gorenstein SDNY*

The Court further finds that the expectation of privacy in movement/location information suggested by these prevalent attitudes is objectively reasonable because historically such information was not observable when someone was within private property and because the newly-emergent technologies create a potential to monitor associational activities in a manner that could have a chilling effect.[69] Finally, the very fact that Congress has taken pains to protect electronically-derived location information from unwarranted disclosure serves independently to make subjectively-held expectations of privacy objectively reasonable.[70]

As discussed above, some Courts have indicated that historic CSLI is routinely obtainable by law enforcement without probable cause and thus have implicitly found no reasonable expectation of privacy therein. In this Court's view, however, the privacy and associational interests implicated are not meaningfully diminished by a delay in disclosure.[71]

The foregoing view of privacy expectations in the context of electronically-derived location information is in keeping with controlling precedent. More particularly, the Supreme Court has effectively recognized, in closely-analogous cases, an individual's reasonable expectation of privacy in information regarding her location when she is on private premises. *Compare United States v. Knotts*, 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983) (concluding that warrantless installation of electronic tracking beeper/radio transmitter inside drum of chemicals sold to the defendant illegal drug manufacturers, and used to follow their movements on public highways, implicated no Fourth Amend-

2005 Opinion (indicating that "most cell users are quite surprised to learn that [CSPs] can create a virtual map" of movements and "are likely to reject the prospect of turning every cell phone into a tracking device"). *Cf. Companies Caught in the Middle*, 21 U.S.F.L.Rev. at 557 ("[W]ith respect to location information ..., many orders now require disclosure of the location of all of the associates who ... made calls to a target.").

69. *Cf. Karo*, 468 U.S. at 714, 104 S.Ct. 3296 ("At the risk of belaboring the obvious, private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable."); *State v. Campbell*, 306 Or. 157, 759 P.2d 1040 (1988) (observing, with regard to warrantless location information, that "freedom may be impaired as much, if not more so, by the treat of scrutiny as by the fact of scrutiny").

70. *Cf. United States v. White*, 401 U.S. 745, 786, 91 S.Ct. 1122, 28 L.Ed.2d 453 (Harlan, J., dissenting) ("Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining the desirability of saddling them upon society. The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens, the risk of the electronic listener or observer without at least the protection of a warrant requirement.").

71. *Cf. State v. Jackson*, 150 Wash.2d 251, 76 P.3d 217, 223–24 (2003) (discussing civil liberties implicated by covert disclosure of "an enormous amount of personal information", and noting, in concluding that GPS device employed by law enforcement was a "particularly intrusive method of surveillance", that the device "provided [Government with] a record of every place the vehicle had been in the past", a feat that no visual surveillance could have accomplished); Matthew M. Werdegar, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 Stan. L. & Pol'y Rev. 103, 105–107 (Fall 1998); *Alexander Mass.2007 Opinion, rev'd, Stearns Mass.2007 Opinion*, 509 F.Supp.2d at 74–75 (dismissing as nonsensical any assertion that an individual's expectation of privacy in her presence at a location that she wished to keep secret is suddenly lost when the activity—or that particularly iteration of the activity—is over and she has left).

ment concerns, as defendants had no reasonable expectation of privacy while they and their vehicle were in plain view on public highways) *with United States v. Karo*, 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984) (concluded that where the tracking beeper placed inside chemical drum was then used to ascertain presence in residences, the search was unreasonable absent probable cause).[72]

Taken together, these cases establish that without a warrant based on probable cause the Government may use a tracking device to ascertain an individual's location on a public highway but not in a private home, *i.e.*, the public/private dichotomy is the principle harmonizing *Knotts* and *Karo*, so that a warrant is constitutionally required if and only if the location information extends onto private property.[73]

But even with this principle as a guide, the Court anticipates that routine allowance of location information up to the threshold of the private domain would necessitate increasingly-difficult line-drawing at the margins. Moreover, even if difficulties in Constitutional line-drawing were surmounted, practical limitations on the abilities of CSPs to filter their CSLI would almost certainly result in over-inclusive disclosures, and thus in transgressions of Constitutional boundaries.[74] Accordingly, these considerations counsel adopting a statutory interpretation which, by retaining the probable cause requirement for all CSLI, would avoid repeated Constitutional adjudication and trespass into protected areas.[75]

The Government has contended, and some Courts have opined, that there is no

72. *See also* 468 U.S. at 711, 104 S.Ct. 3296 (" 'All individuals have a legitimate expectation of privacy that objects coming into their rightful ownership do not ... give law enforcement agents the opportunity to monitor [their] location ... inside private residences and other areas where the right to be free from warrantless governmental intrusion is unquestioned.' ").

73. *Cf., e.g., McGiverin PR 2007 Opinion*, 497 F.Supp.2d at 311–12 ("[T]he warrantless monitoring of a tracking device does not offend the Fourth Amendment so long as the situs of the thing being tracked could be determined by visual observation from a public area and ... the surveillance tells authorities nothing about the suspect's location within an area ... where he/she enjoys a reasonable expectation of privacy.").

74. The Court does not believe that these difficulties can be met by reliance on investigative agencies' self-restraint. *See United States v. United States Dist. Ct.*, 407 U.S. 297, 317, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972) (Powell, J.) (concluding that the "Fourth Amendment contemplates a prior judicial judgment", and not the "risk that executive discretion may be reasonably exercised"). *Feldman WDNY 2006 Opinion*, 415 F.Supp.2d at 217–19 & n. 5 (discussing Government's "shifting" position on what standard applies to CSLI as paying "tribute ... to the slippery constitutional slope [its] position involves"), *id.* at 218 n. 5 (quoting law enforcement agent's testimony that the Government was "back[ing] off" and requesting *limited* CSLI in response to Magistrate Judges' privacy concerns and in interests of avoiding "a hell of a fight" on the "slippery ground" of the applicability "of a probable cause standard"). *See* 407 U.S. at 317, 92 S.Ct. 2125 (Magistrate Judges' role "accords with our basic constitutional doctrine that individual freedoms will be best preserved through a separation of powers and division of functions among the different branches and levels of government").

75. *See Karo*, 468 U.S. at 717, 104 S.Ct. 3296 (assessing Government's argument that, if warrants are required when a location-identifying device is not in public view, then "for all practical purposes [agents] will be forced to obtain warrants in every case in which they seek to use [a tracking device], because they have no way of knowing in advance whether [it] will be transmitting its signals from inside private premises"); *id.* (concluding that "[t]he argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement").

Cf. Smith SD Tex 2005 Opinion, 396 F.Supp.2d at 757 (concluding, in discussion of Fourth Amendment implications: "For purposes of this decision it is unnecessary to draw the line between permissible and impermissible warrantless monitoring of [CSLI]. As

reasonable 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*.[76] As explained by Magistrate Judge Smith, the Sixth Circuit has expressly (and in this Court's view correctly) rejected this less apt analogy:

> The government contends that probable cause should never be required for cell phone tracking because there is no reasonable expectation of privacy in [CSLI], 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). The Sixth Circuit rejected that analogy in *United States v. Forest*, 355 F.3d 942, 951–52 (6th Cir.2004). Unlike dialed telephone numbers, [CSLI] is not 'voluntarily conveyed' by the user to the phone company.... [I]t is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge. Sometimes, as in *Forest*, [CSLI] is triggered by law enforcement's dialing of the particular number. 355 F.3d at 951. For these reasons the Sixth Circuit was persuaded that *Smith* did not extend to [CSLI], but rejected the defendant's constitutional claim on the narrower ground that the surveillance took place on public highways, where there is no legitimate expectation of privacy. *Id.* at 951–52 (citing *United States v. Knotts*, 460 U.S. 276, 281, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983)).

Smith SD Tex.2005 Opinion, 396 F.Supp.2d at 756–573.

A panel of the Sixth Circuit more recently further elucidated the bounds of the waiver of expectation doctrine in *Warshak*, 490 F.3d 455,[77] in which it explained that if

in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights. The mere possibility of such an invasion is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant. 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.")

It also appears that Congress, in expressly excepting tracking device communications and location information from the various provisions of its electronic communications legislation, intended to provide an ample zone of protection for Fourth Amendment rights. *Cf. Clark v. Martinez*, 543 U.S. 371, 381, 125 S.Ct. 716, 160 L.Ed.2d 734 (2005) (canon of constitutional avoidance is grounded on presumption that Congress did not intentionally "raise[ ] serious constitutional doubts").

76. In concluding that there is no reasonable expectation of privacy in the dialed telephone phone numbers obtained through a Trap and Trace, the Court relied on *United States v. Miller*, 425 U.S. 435, 442, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (banking records obtained by subpoena not suppressed; no reasonable expectation of privacy because knowingly and voluntarily conveyed to bank employees for transactional use). *Cf.* Jack X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, PLI Order No. 11253, 420–21 (June–July 2007) (observing that the *Smith* Court "stressed the narrowness of its ruling" and that the assumption of the risk/business records doctrine "was developed when courts did not foresee" the revealing nature or quantity of information now stored by communications service providers).

77. This decision—affirming with "minor modification" the District Court's entry of a preliminary injunction on grounds of the facial constitutional flaws of a statutory interpretation authorizing seizure of personal e-mails from service provider based only on Government's *ex parte* representations of less than probable cause—was vacated and rehearing *en banc* on this novel question granted by the Sixth Circuit in October, 2007.

an intermediary's mere ability to access information sought by the Government was enough to create an assumption of the risk bar to a reasonable expectation of privacy, vast stores of personal information would lose their Constitutional protections.[78] Because such consequences are clearly unacceptable under the Fourth Amendment, the Sixth Circuit concluded that the "critical question" is "whether a [customer] maintains a reasonable expectation of privacy in [the information sought] *vis-a-vis* the [third-party provider]". 490 F.3d at 469. The Court concluded, largely on its analysis of *Katz*, *Miller* and *Smith*, that a customer forfeits her reasonable expectation of privacy only as to a service provider's records of information voluntarily conveyed and reasonably expected to be accessed by the provider's employees in the ordinary course of its business (*i.e.*, for purposes of the provision of services). *See id.* at 469–76.

As discussed *supra*, CSLI is not "voluntarily and knowingly" conveyed by cell phone users (certainly *not* in the way of transactional bank records or dialed telephone numbers); rather, the information is automatically registered by the cell phone.[79] Nor are CSP employees routinely reviewing and/or utilizing CSLI in the ordinary course of the provision of telephone communications services; rather, the information is processed on separate control channels by electronic equipment.[80] Nor does a CPS's retention of CSLI generally serve any business purpose for the customer or for the provider in serving the customer; rather, such information is retained principally, if not exclusively, in response to Government directive.[81]

Finally, the movement/location information at issue here, unlike the records found unprotected in prior Supreme Court cases, is the subject of express Congressional protection. Indeed, Congress has reiterated throughout the legislative history of its electronic communications legislation, and reflected in the provisions of its enactments, its recognition of an individual expectation of privacy in "location information" and desire to protect this privacy

78. *See* 490 F.3d at 470 (concluding that, if privacy expectations were deemed waived as to information a third-party "has the ability to access", phone conversations, letters, and the contents of third-party storage containers would all be unprotected).

79. *See United States v. Forest*, 355 F.3d 942, 949 (6th Cir.2004) (finding that defendant "persuasively distinguishe[d]" CSLI, which was not "voluntarily convey[ed] ... to anyone", from dialed telephone numbers in *Smith v. Maryland*).

80. *Compare id.* at 949 (noting that CSLI is "simply data sent from a cellular phone tower to the cellular provider's computers") *with Miller*, 425 U.S. at 442, 96 S.Ct. 1619 (because bank customers knowingly permitted bank employees to view records of financial transactions, they had no "legitimate expectation of privacy"). *See Warshak*, 490 F.3d at 473–75 (contrasting "mere accessibility" with service that includes routine "inspection, auditing, or monitoring" and contrasting electronic processing/scanning of information with "manual human review").

81. *Azrack E.D.N.Y.2007 Opinion*, 2007 WL 2729668 at *11 (noting, in distinguish *Miller* and *Smith*, that the information at issue *sub judice* was neither kept in the ordinary course of business nor contained on the user's monthly bill).

The Government cannot, of course, remove an otherwise reasonable expectation of privacy by mandating that it have the ability to intrude. *Cf. Smith*, 442 U.S. at 739 n. 5, 99 S.Ct. 2577 (observing that Fourth Amendment protections cannot be erased by Government's disclosure of its access to particular information). *First Practices*, 2007 Stan. Tech. L.Rev. at 26 (noting in discussing *Katz*: "That law enforcement agents have the technical capability to access [electronic communication information], cannot mean that a user assumes the risk that agents will access whatever ... they choose, independent of any judicial oversight.").

right from unwarranted or unreasonable encroachment.

In sum, this Court concurs with the assessment of Magistrate Judge Smith at the conclusion of his Opinion:

> Denial of the government's request ... in this instance should have no dire consequences for law enforcement [as t]his type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41. On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected.... Absent any sign that Congress has squarely addressed and resolved those concerns in favor of law enforcement, the more prudent course is to avoid an interpretation that risks a constitutional collision.

Smith SD Tex.2005 Opinion, 396 F.Supp.2d at 765 (citation omitted).[82]

VI. CONCLUSION

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.Civ.P. 41, must be denied. This Opinion is joined, in the interest of judicial efficiency, by Magistrate Judges Caiazza, Hay, Baxter and Mitchell.[83]

ACCORDINGLY, IT IS HEREBY ORDERED THAT

The application of the Assistant United States Attorney be denied, except that the underlying application be sealed as requested by the Government in order not to jeopardize an ongoing criminal investigation.

This Opinion shall not be sealed because it is a matter of first impression in this District and Circuit on issues concerning the statutory and Constitutional regulation of electronic surveillance which do not hinge on the particulars of the underlying investigation.

CONTECH STORMWATER SOLUTIONS, INC.

v.

BAYSAVER TECHNOLOGIES, INC., and Accubid Excavation, Inc.

Civil Action No. CCB–07–358.

United States District Court, D. Maryland.

Jan. 15, 2008.

Background: Patent owner brought action against competitors alleging infringement. Competitors counterclaimed asserting business tort theories and pat-

82. *See also Almeida–Sanchez v. United States*, 413 U.S. 266, 273, 93 S.Ct. 2535, 37 L.Ed.2d 596 (1973) ("The needs of law enforcement stand in constant tension with the Constitution's protections of the individual against certain exercises of official power. It is precisely the predictability of these pressures that counsels a resolute loyalty to constitutional safeguards.").

83. *See Robinson DDC 2005 Order, supra* n. 61 (denying, on behalf of Magistrate Judges Robinson, Kay and Facciola, Government's applications for Orders authorizing the disclosure of CSLI by authority under either § 2703, §§ 3122 and 3123, or both, absent a showing of probable cause).

~~SECRET~~

Classified by: [redacted] Assistant Attorney General, NSD, DOJ

Reason: 1.4(c)

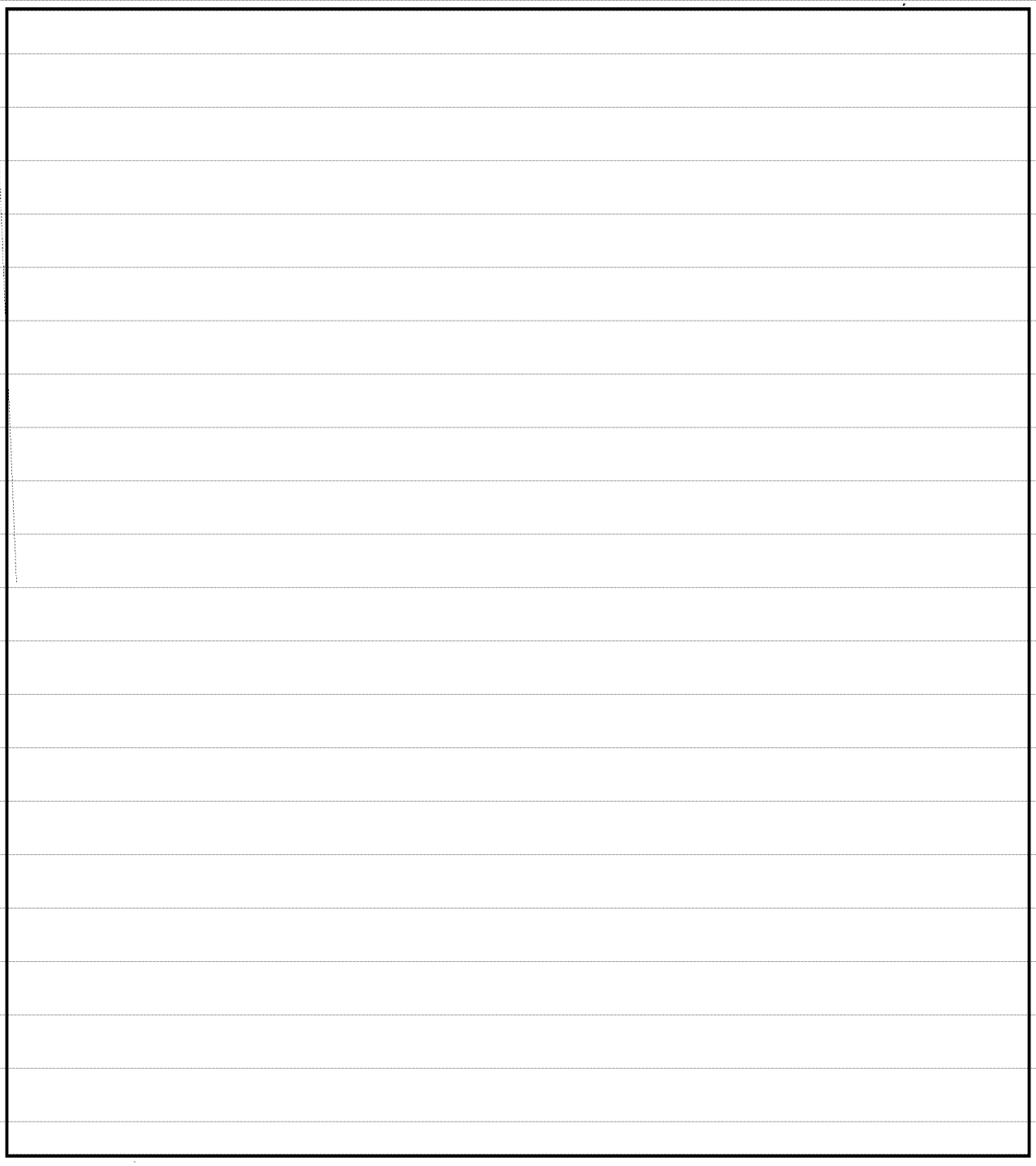
Declassify on: 2 March 2036

b6
b7C

~~SECRET~~

~~SECRET~~//REL TO FVEY//20360603

(S)



b1
b3
b7E

~~SECRET~~//REL TO FVEY//20360603

~~SECRET~~

DATE: 11-08-2012
CLASSIFIED BY 65179 DMH/rs
REASON: 1.4 (c)
DECLASSIFY ON: 11-08-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b3
b6
b7C
b7E

From:
Sent: Monday, August 30, 2010 2:44 PM
To:
Cc:
Subject: (U) FW: (S//NF) Matters: PAMS Reporting and Future Funding

~~SECRET~~//NOFORN
RECORD

~~SECRET~~//NOFORN
RECORD

Project Leads,

(U) (S//NF) I've been meeting recently with TMSU and evaluating the effectiveness of our current Project Managements controls (e.g. PAMS) in meeting the expectations of the We observed that the level of reporting varied widely and determined that the level of detail for some projects was insufficient to assess the health or status of the particular project.

(U//FOUO) In response, we have prepared the following information to guide you in completing the PAMS reporting for your projects:

(U/FOUO) Reporting Activities in PAMS

b5

(U)

PAMS-Chart.doc

(Attachment: "Standards for Reporting of Activities in PAMS"- Filename: PAMS-Chart.doc)

(S)

b1
b3
b5

(U/FOUO) Future Funding Concerns

CELL/OTD 012463

~~SECRET~~

b1
b3
b5
b7E

(S)

(U) (S//NF) The collective impact will present many challenges as base funding is reduced and agencies compete for enhancement monies via alternative sources such as the Meanwhile, the effort could itself have rescissions to deal with. Anticipating an appropriate response to future funding shortfalls and planning accordingly will be the FBI's best strategy for ensuring that it derives the maximum benefit from financial resources sources that do remain available.

(U//FOUO) The FBI strategy is broken down into

b5

(S)

b1
b3
b5

b5

(U) I ask all project leads to keep this strategy in mind as you move forward and begin preparing your project briefings for November. If you have any questions, please contact me at your convenience.

Sincerely,

b6
b7C

FBI OTD

DERIVED FROM: Multiple Sources
DECLASSIFY ON: 20350830
~~SECRET~~//NOFORN

~~SECRET~~

DATE: 11-13-2012
CLASSIFIED BY 65179 DMH/rs
REASON: 1.4 (c, g)
DECLASSIFY ON: 11-13-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b6
b7C
b7E

From:
Sent: Thursday, August 12, 2010 1:15 PM
To:
Subject: FW: Field Demo Summary

~~SECRET//NOFORN~~
RECORD

See below.

From:
Sent: Friday, July 09, 2010 2:01 PM
To:
Cc:
Subject: Field Demo Summary

~~SECRET//NOFORN~~
RECORD

The attendees are as follows:

FBI

b6
b7C
b7E

This is a follow-up to the Bureau visit to office last month in the preliminary evaluation of

b1
b3
b5
b7E

(S)

~~SECRET~~

CELL/OTD 007788

(S)

b1
b3
b5
b7E

DERIVED ~~FROM~~: Multiple Sources
DECLASSIFY ON: 20350709
SECRET//NOFORN

DERIVED ~~FROM~~: Multiple Sources
DECLASSIFY ON: 20350709
SECRET//NOFORN

DERIVED ~~FROM~~: Multiple Sources
DECLASSIFY ON: 20350709
SECRET//NOFORN

DATE: 11-13-2012
CLASSIFIED BY 65179 DMH/rs
REASON: 1.4 (c)
DECLASSIFY ON: 11-13-2037

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE b3 b6 b7C b7E

From:
Sent: Thursday, July 13, 2006 11:18 AM
To:
Cc:
Subject: EC from

~~SECRET~~//NOFORN
RECORD 66f-hq-1410124f

As we discussed last week, I emailed and asked for a copy of the EC that submitted to OTD for additional sent me the attached EC, which was uploaded on the system around the end of June.

OTD.Equipment.Request EC.wpd

b3 b7E

(S) b1 b3 b5 b7E

(S) FBI/OTD

Unclass email:

(S) b1 b3 b6 b7C

Non-Secure
Stu3
Cell
Pager

CLASSIFIED BY: 74484,OTD/FO,OTD
REASON: 1.5[c]
DECLASSIFY ON: 20160713
SECRET//NOFORN

CELL/OTD 007905

(Rev. 01-31-2003)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY **Date:** 06/28/2006

To: [redacted] b6 b7C b7E

OTD **Attn:** AD Kerry E. Haynes,
UC [redacted]
SSA [redacted]

[redacted] b6 b7C b7E

[redacted]

b6
b7C
b7E

From: Criminal Investigative
VCS/VCU, Room [redacted]
Contact: [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: 62F-HQ-C1522631 (Pending)
7C-HQ-C1510131

Title: CRIMINAL INVESTIGATIVE DIVISION (CID);
Violent Crime - [redacted]

[redacted]

VIOLENT CRIMES PROGRAM

Synopsis: Request necessary equipment to facilitate outfitting [redacted] additional [redacted]

Details: For information, the captioned initiative was approved by A/EAD [redacted], A/AD [redacted], and AD Kerry E. Haynes to assist violent crimes supervisors with [redacted] These facts, coupled with violent crimes investigations remaining a number eight priority in the FBI, place an extreme burden on violent crimes resources.

b3
b6
b7C
b7E

CID/VCU, working closely with OTD and CID/CACU, recently coordinated the purchase of [redacted]

CID's original [redacted] members have received extensive [redacted] To facilitate the fielding of

b3
b7E

As of 06/16/2006, CID coordinated the training of additional members from the following offices:

Accordingly, CID requests OTD to identify all appropriate supporting equipment, to support the newly trained Should listed equipment not be available through OTD, CID requests OTD consider the loan of additional equipment until such time CID can fund the additional purchase of equipment.

b3
b7E

LEAD(S):

b7E

[redacted]

OPERATIONAL TECHNOLOGY DIVISION

AT QUANTICO, VA

CID requests OTD to identify [redacted] all appropriate supporting equipment, [redacted] to support the newly trained [redacted] Should listed equipment not be available through OTD, CID requests OTD consider the loan of additional equipment until such time CID can fund the additional purchase of equipment. b3 b7E

[redacted]

[redacted]

b7E

Read and clear.

CC: 1- Executive Staff for Strategic
Planning and Coordination
1- Special Assistant to the AD

♦♦