UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone

460 F. Supp. 2d 448
2006 U.S. Dist. Lexis 76822

October 23, 2006, Decided
October 23, 2006, Filed

MEMORANDUM OPINION

LEWIS A. KAPLAN, *District Judge.*

The question before the Court is whether the government may obtain, without a showing of probable cause, prospective cell site information that would reveal the general location -- and, in some circumstances, permit law enforcement agents to track the precise movements -- of a particular cellular telephone on a real-time basis. The government contends that courts may order the disclosure of such information pursuant to the combined authority of 18 U.S.C. § 3121 *et seq.* (the "Pen Register Statute") and 18 U.S.C. § 2701 *et seq.* (the "Stored Communications Act").

Although there is little indication that Congress actually intended that the Pen Register Statute and the Stored Communications Act could be combined to authorize the disclosure of prospective cell site information, the language of the two statutes, when read together, clearly authorizes such disclosure. The Court is bound to follow such clear statutory language. Congress nevertheless may wish to consider whether this result is consistent with its intention.

Background

A. Cell Site Information

Cellular telephone networks are divided into geographic coverage areas known as "cells," which range in diameter from many miles in suburban or rural areas to several hundred feet in urban areas. [1] Each contains an antenna tower, one function of which is to receive signals from and transmit signals to cellular telephones.

1 *In re Application of the United States of America for an Order for Disclosure of Telecomm. Records and Authorizing the Use of A Pen Register and Trap and Trace*, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005) (the *"S.D.N.Y. I Decision"*); Gov. Br. 3.

Whenever a cellular telephone is in the "on" condition, regardless of whether it is making or receiving a voice or data call, it periodically transmits a unique identification number to register its presence and location in the network. That signal, as well as calls made from the cellular phone, are received by every antenna tower within range of the phone. When the signal is received by more than one tower, the network's switching capability temporarily "assigns" the phone to the tower that is receiving the strongest signal from it. As a cellular telephone moves about, the antenna tower receiving the strongest signal may change as, for example, often occurs when a cellular phone moves closer to a different antenna tower. At that point, the cellular telephone, including any call in progress, is assigned to the new antenna tower. [2]

2 Failures in this handing off function doubtless account for a great many of the "dropped calls" that so aggravate cellular telephone users.

The location of the antenna tower receiving a signal from a given cellular telephone [*451] at any given moment inherently fixes the general location of the phone. Indeed, in some instances, depending upon the characteristics of the particular network and its equipment and software, it is possible to determine not only the tower receiving a signal from a particular phone at any given moment, but also in which of the three 120-degree arcs of the 360-degree circle surrounding the tower the particular phone is located. In some cases, however, the available information is even more precise.

Often, especially in urban and suburban areas, the signal transmitted by a cellular telephone is received by two or more antenna towers simultaneously. Knowledge of the locations of multiple towers receiving signals from a particular telephone at a given moment permits the determination, by simple mathematics, of the location of the telephone with a fair degree of precision through the long established process known as triangulation. [3] Real time information concerning the location permits the geographic movements of the phone to be tracked as they occur.

3 Triangulation is the process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points. While only the length of one side of the triangle is known at first (the side connecting the two known points), simple trigonometry reveals the lengths of the other sides and so the position of the third point. In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information about which face of each tower is facing the phone.

Another method of tracking the location of cellular telephones, which also is sometimes called triangulation, is possible when a phone transmits signals to three antenna towers at once. Based on the strength of a phone's signal to a tower, and the time delay for the signal to reach the tower, one can determine the distance between the

phone and the tower. One can then draw around the tower a circle, the radius of which is the distance from that tower to the phone. The location of the phone can be pinpointed by drawing circles around three of more towers and seeing where the circles intersect.

Cellular telephone service providers record the identity and location of the antenna towers receiving signals from each phone at every point in time. As noted, some record also which 120-degree face or sector of the tower faces the phone. Some record also the identities and locations of all antenna towers receiving signals from each phone at every moment.

This information, referred to collectively here as "cell site information," usually serves rather benign purposes, such as determining whether roaming charges apply and tracking call volume by location. [4] But the information is capable of another use.

4 *See In re Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 949-50 (E.D. Wisc. 2006) (the *"Wisconsin Decision"); S.D.N.Y. I Decision*, 405 F. Supp. 2d at 436-37; Gov. Br. at 2-3.

In recent years, law enforcement officials have begun to seek cell site information in applications for the installation and use of pen registers and trap and trace devices (i.e., devices that record the numbers dialed from or calling a particular telephone). [5] According to the government, [*452] "cell site information is an important investigatory tool which is used . . . to, among other things, help determine where to establish physical surveillence and to help locate kidnapping victims, fugitives, and targets of criminal investigations." [6]

5 As Judge Gorenstein noted in an opinion authorizing the disclosure of prospective cell site data, although these terms historically referred to physical devices that recorded call information for a particular telephone, it is not always necessary to install a physical device on a telephone line to obtain such information, which "can now be transmitted digitally by the telephone service providers" in many cases. *S.D.N.Y. I Decision*, 405 F. Supp. 2d at 439 n.1. Nevertheless, the government "is bound to follow the Pen Register Statue to obtain information otherwise covered by the statute." *Id.*

6 Gov. Br. 2.

Its usefulness for these purposes depends largely upon the number of antenna towers from which the government obtains information at a given time. Where the law enforcement agents obtain information from only one tower at a time, they can determine that a cell phone is in the cell served by that tower and, in some cases, which sector of the tower faces the cell phone; but they can neither pinpoint the precise location of the cell phone nor track its movements. Where, however, the government obtains information from multiple towers simultaneously, it often can triangulate the caller's precise location and movements by comparing the strength, angle, and timing of the cell phone's signal measured from each of the sites. [7]

7 *S.D.N.Y. I Decision*, 405 F. Supp. 2d at 438; *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info.*, 396 F. Supp. 2d 294, 300 (E.D.N.Y. 2005) (the *"E.D.N.Y. Decision"*).

Many of the initial applications for cell site information sought information that could be used for triangulation. [8] After these applications were rejected by many courts, however, the government began to request information regarding only one tower at a time, apparently in the hope that applications for less detailed and invasive information would meet with a warmer judicial reception. [9] This application is part of the latter group, seeking the identity of only one tower receiving transmissions -- presumably the tower receiving the strongest signal -- from the subject telephone at a particular time. The government's arguments for statutory authorization, however, apply equally whether information is obtained from one antenna tower at a time or from many simultaneously. [10] In other words, if the Pen Register Statute and the Stored Communications Act together authorize the disclosure of cell site information from a single antenna tower, there is no reason to believe that they would not authorize disclosure of such information from multiple antenna towers simultaneously.

8 *See, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) (the *"Texas Magistrate Decision"*); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys on Tel. Nos. (Sealed) and the Production of Real Time Cell Site Info.*, 402 F. Supp. 2d 597, 599 (D. Md. 2005) (the *"Maryland I Decision"*).

9 *See, e.g., S.D.N.Y. I Decision*, 405 F. Supp. 2d at 438; *Wisconsin Decision*, 412 F. Supp. 2d at 951.

10 *Wisconsin Decision*, 412 F. Supp. 2d at 951; *Amicus* Br. 26-27.

B. Prior Opinions

To date, at least three district and eleven magistrate judges have issued opinions addressing applications for orders authorizing the disclosure of prospective cell site information pursuant to the Pen Register Statute and the Stored Communications Act. The majority of the magistrate judges, as well as district judge in the Northern District of Indiana [11] and the [*453] Eastern District of Wisconsin, [12] denied the government's requests, concluding that "statutory authority for prospective cell site location information is lacking." [13] Three of the magistrate judge opinions, however, including a comprehensive analysis by Magistrate Judge Gorenstein in this district, held that the Pen Register Statute and the Stored Communications Act, read in conjunction, authorize the disclosure of prospective cell site information. [14] At least one district judge has reached the same conclusion. [15]

11 *In the Matter of the Application of the United States of America for an Order (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs.; In the Matter of the Application of the United States of America for an Order (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Location of Cell Site Origination and/or Termination*, 2006 U.S. Dist. L exis 45643, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. Jul. 5, 2006) (Lee, J.) (the *"Indiana Decision"*).

12 *In re United States for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp. 2d 947, 2006 WL 2871743 (E.D.Wis. Oct. 6, 2006) (Adelman, J.) (affirming *Wisconsin Decision*).

13 *In re Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 2006 U.S. Dist. L exis 11747, No. 06 Crim. Misc. 01, 2006 WL 468300, *2 (S.D.N.Y. Feb. 28, 2006) (Peck, M.J.) (the *"S.D.N.Y. II Decision"); see also In Matter of Application for an Order Authorizing the Installation and use of a Pen Register and Directing the Disclosure of Telecomms. Records for Cellular Phone assigned the No. [Sealed]*, 439 F. Supp. 2d 456, 457 (D. Md. 2006) (Bredar, M.J.); *In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (Smith, M.J); *In the Matter of the Application of the United States of America for an Order (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Info.; and (3) Authorizing the Disclosure of Location-Based Servs., Nos. 1:06-MJ-23, 1:-6-MJ-24, slip op. (N.D. Ind. May 17, 2006) (M.J.), superceded by the* Indiana Decision, 2006 U.S. Dist. L exis 45643, 2006 WL 1876847; *In re Applications of the United States for Orders Authorizing the Disclosure of Cell Cite Info.*, 2005 U.S. Dist. L exis 43736, Nos. 05-403 et al., 2005 WL 3658531 (D.D.C. Oct. 26, 2005) (Robinson, M.J.); *In re Application of the United States for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Tel. Nos. [Sealed] and [Sealed]*, 416 F. Supp. 2d 390 (D. Md. 2006) (Bredar, M.J.) (the "Maryland II Decision"); *In re Application of the United States For An Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace and the Disclosure of Subscriber and Activity Info. Under 18 U.S.C. § 2703*, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) (Feldman, M.J.) (the *"W.D.N.Y. Decision"*); *In re Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info.*, 407 F. Supp. 2d 134 (D.D.C. 2006) (Facciola, M.J.); *Wisconsin Decision*, 412 F. Supp. 2d at 949 (Callahan, M.J.); *E.D.N.Y. Decision*, 396 F. Supp. 2d at 295 (Orenstein, M.J.); *Maryland I Decision*, 402 F. Supp. 2d at 605 (Bredar, M.J.); *Texas Magistrate Deci-*

sion, 396 F. Supp. 2d at 765 (Smith, M.J.); *see also In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register with Caller Identification Device and Cell Site Location Authority on a Certain Cellular Tel.,* 415 F. Supp. 2d 663, 665-66 (S.D. W.Va. 2006) (Stanley, M.J) (expressing doubt that the Pen Register Statute and the Stored Communications Act authorize disclosure of cell site information where the target user is the owner of the cell phone, but holding that those statutes do authorize such disclosure where the user is a fugitive who is not the owner of the phone).

14 *See S.D.N.Y. I Decision,* 405 F. Supp. 2d at 448-49 (Gorenstein, M.J.); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device and Authorizing Release of Subscriber Info. and/or Cell Site Info.,* 411 F. Supp. 2d 678 (W.D. La. Jan, 26, 2006) (Hornsby, M.J.); In re Application for an Order Authorizing the Installation and Use of a Pen Register Device, Trap and Trace Device, Dialed No. Interceptor, No. Search Device, and Caller Identification Serv., and the Disclosure of Billing, Subscriber, and Air Time Info., No. S-06-SW-0041, slip op. (E.D. Cal. Mar. 15, 2006) In re Application for an Order Authorizing the Installation and Use of a Pen Register Device, Trap and Trace Device, Dialed No. Interceptor, No. Search Device, and Caller Identification Serv., and the Disclosure of Billing, Subscriber, and Air Time Info., No. S-06-SW-0041, slip op. (E.D. Cal. Mar. 15, 2006) (M.J).

15 *See In re Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Info.,* 433 F. Supp. 2d 804 (S.D. Tex. 2006) (the *"Texas District Decision"*).

[*454]

C. This Application

On February 22, 2006, the government applied to Magistrate Judge Andrew J. Peck for an order authorizing the use of a pen register and trap and trace device to capture the calls made and received by a particular cellular telephone. [16] The government requested that the order further authorize the pen register

> "to capture and report at the same time originating and terminating cell site location information (specifically, information which identifies the antenna tower receiving transmissions from that cellphone . . . and any information on what portion of that tower is receiving a transmission . . . at the beginning and end of a particular telephone call made or received by the cellphone's user, which information is to be transmitted from the cellphone's service provider to the DEA and other law enforcement agencies) . . ., for all calls made to or from the [cellphone]." [17]

Judge Peck denied the government's application, adopting what he deemed the majority view set forth in the cases described above. [18] On March 17, 2006, the government renewed its application before the undersigned. [19] The Court invited the Federal Defenders of New York to appear as *amicus curiae.*

16 *S.D.N.Y. II Decision*, 2006 WL 468300 at *1 (quoting the government's sealed application).

17 *Id.* (quoting the government's sealed application).

18 *Id.* at 4 (internal quotation marks omitted).

19 The undersigned was serving in Part I at the time.

Discussion

A. The Government's Theory

The government makes a three part argument in support of its application. First, it asserts that the Pen Register Statute permits courts to order the installation of pen registers and trap and trace devices that, in addition to reporting the telephone numbers of incoming and outgoing calls made from a particular cell phone, would disclose also the cell site information for the beginning and end of each call. It acknowledges that the Communications Assistance for Law Enforcement Act of 1994 [20] ("CALEA") requires that courts rely also on some additional statutory authority when ordering the disclosure of prospective cell site information under the Pen Register Statute. Finally, it contends that the Stored Communications Act provides the additional authority required by CALEA.

20 47 U.S.C. 1001 *et seq.*

1. The Pen Register Statute

The government first contends that the Pen Register Statute, when accompanied by the additional authority discussed below, permits courts to order the installation of pen registers and trap and trace devices that provide not only the telephone numbers of incoming and outgoing calls made from a particular cell phone, but also the cell site information for the beginning and end of each call.

As always, the starting point in construing a statute must be its text. [21] The Pen [*455] Register Statute provides, with certain exceptions not relevant here, that "no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title." [22] Section 3123 authorizes a court to enter an *ex parte* order permitting telephone service providers or law enforcement officials to install and use these

devices upon an application by the government certifying that "information likely to be obtained from such installation and use is relevant to an ongoing criminal investigation." [23]

21 *E.g., Saks v. Franklin Covey Co.*, 316 F.3d 337, 345 (2d Cir. 2003).

22 18 U.S.C. § 3121(a).

23 18 U.S.C. § 3123.

When the statute was enacted in 1986, pen registers and trap and trace devices were given "narrow definitions limited to the capture of telephone numbers." [24] The USA PATRIOT Act of 2001 (the "Patriot Act"), however, significantly broadened the definitions of these terms. A "pen register" is now defined as

> "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." [25]

Similarly, a "trap and trace device" now refers to

> "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." [26]

24 *Maryland II Decision*, 416 F. Supp. 2d at 394-95.

25 18 U.S.C. § 3127(3).

26 18 U.S.C. § 3127(4).

The amended definitions encompass the cell site information the government seeks here. [27] As discussed above, a cell phone transmits signals to the nearest antenna tower or towers when the user makes a call. This information is "signaling information" within the meaning of the Pen Register Statute.

27 As noted above, the government here seeks information identifying the antenna tower receiving transmissions from the subject telephone at the beginning and end of particular telephone calls. The Court need not determine whether the term "signaling information" includes also transmissions made by cell phones in between calls to register their presence in the network, as the government does not seek such information here. *See S.D.N.Y. I Decision*, 405 F. Supp. 2d at 439 n. 2.

A number of the judges to address this issue have reached the same conclusion, even several who ultimately denied applications for cell site information for other reasons. [28] This interpretation finds further support in *United States Telecom Association v. FCC,* [29] in which the Court of Appeals for the District of Columbia Circuit held that cell site information constituted "signaling information" under CALEA. The court explained that "a mobile phone sends signals to the nearest cell site at the start and end of a call. These signals, which are necessary to achieve communications between the caller and the party he or she is calling, clearly are 'signaling information.'" [30]

28 *Indiana Decision,* 2006 U.S. Dist. L exis 45643, 2006 WL 1876847 at *1; *Maryland II Decision,* 416 F. Supp. 2d at 394; *S.D.N.Y. I Decision,* 405 F. Supp. 2d at 438-39; *W.D.N.Y. Decision,* 415 F.Supp.2d at 214; *Wisconsin Decision,* 412 F. Supp. 2d at 953.

29 343 U.S. App. D.C. 278, 227 F.3d 450 (D.C. Cir. 2000).

30 *Id.* at 463-64.

[*456] At least two of the magistrate judges have come to the opposite conclusion, asserting that "nothing in the [Patriot Act's] legislative history suggests that anyone . . . contemplated that the addition of 'dialing, routing, addressing, and signaling information' to the definition of pen/trap devices would extend the reach of such devices to capture cell site information." [31] Instead, according Magistrate Judge Smith in the Southern District of Texas, "the PATRIOT Act's expansion of the pen/trap definitions was intended only to reach electronic communications such as email." [32]

31 *E.D.N.Y. Decision,* 396 F. Supp. 2d at 318; *Texas Magistrate Decision,* 396 F. Supp. 2d at 761-62.

32 *Texas Magistrate Decision,* 396 F. Supp. 2d at 761.

This argument is unpersuasive for several reasons. First, the language of the statute is clear on its face and contains no limitation to electronic communications such as email. Courts "do not resort to legislative history to cloud a statutory text that is clear," even in the face of "contrary indications in the statute's legislative history.'" [33] Further, the House Report on the Patriot Act indicates that Congress did intend the new definitions of pen registers and trap and trace devices to apply to all communications media, not just email. [34] And even without this evidence of legislative intent, the Court presumes that Congress knew -- when it added the term "signaling information" to the definitions of pen registers and trap and trace devices in 2001 -- that the D.C. Circuit had interpreted that term to include cell site information in the *United States Telecom Association* decision a year earlier. [35] Nothing in the legislative history indicates that Congress intended to abrogate the D.C. Circuit's interpretation of "signaling information."

33 *County of Suffolk v. First Am. Real Estate Solutions*, 261 F.3d 179, 190 (2d Cir. 2001) (quoting *Ratzlaf v. United States*, 510 U.S. 135, 147-48, 114 S. Ct. 655, 126 L. Ed. 2d 615 (1994)); *cf. Chrzanoski v. Ashcroft*, 327 F.3d 188, 196 (2d Cir. 2003) (quoting *Dep't of Housing & Urban Dev. v. Rucker*, 535 U.S. 125, 122 S. Ct. 1230, 152 L. Ed. 2d 258 (2002)).

34 Indeed, the report notes that the amendments to the Pen Register Statute clarified

> "that orders for the installation of pen register and trap and trace devices may obtain *any non-content information* -- 'dialing, routing, addressing, and signaling information' -- utilized in the processing or transmitting of wire and electronic communications. . . [The limitation that] the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media*, and to actual connections as well as attempted connections (such as busy signals and similar signals in the telephone context and packets that merely request a telnet connection in the Internet context)." H.R.REP. NO. 107-236(I), at 53 (2001), *available at* 2001 WL 1205861; *see also S.D.N.Y. I Decision,* 405 F. Supp. 2d at 439.

35 *See Lorillard v. Pons*, 434 U.S. 575, 581, 98 S. Ct. 866, 55 L. Ed. 2d 40 (1978) ("Where . . . Congress adopts a new law incorporating sections of a prior law, Congress normally can be presumed to have had knowledge of the [administrative or judicial] interpretation given to the incorporated law, at least as it affects the new statute.")

2. CALEA

The next prong of the government's argument focuses on Section 1002 of CALEA, which requires telecommunications carriers to ensure that their equipment is capable of, among other things,

> "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier . . . except that, with regard to information [*457] acquired *solely pursuant to the authority for pen registers and trap and trace devices* (as defined in section 3127 of Title 18), 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)." [36]

36 47 U.S.C. 1002(a)(2) (emphasis added).

The government concedes that cell site information is "information that may disclose the physical location of the subscriber" and that the "solely pursuant" clause prevents it from

obtaining such information pursuant to the Pen Register Statute alone. It contends, however, that Section 1002 does not bar the disclosure of cell site information under the Pen Register Statute altogether, but instead permits such disclosure "pursuant to a combination of the [Pen Register Statute] and some other authority." [37] *Amicus* contends that Section 1002 does not authorize the government's hybrid approach. [38]

37 Gov. Br. 14-15.

38 *Amicus* Br. 3-5.

Again, the starting point is the statutory text. [39] Here, the analysis turns on the meaning of the words "solely pursuant." [40] As Judge Gorenstein noted, "'solely' means 'without another' or 'to the exclusion of all else.'" [41] Accordingly, the most natural reading of Section 1002(a)(2) is that cell site information may not be disclosed pursuant to the Pen Register Statute alone without authorization by some other statutory provision. It follows that cell site information may be disclosed pursuant to the Pen Register Statute *and* some additional statutory authority. In other words, Section 1002 does not prevent courts from authorizing the disclosure of cell site information under the Pen Register Statute. It merely requires additional statutory authority for any such order. [42]

39 It is possible to read the exception clause in Section 1002(a)(2) as referring to the kinds of capabilities a telecommunications provider is required to possess, rather than the kinds of information a carrier should disclose to the government pursuant to a court order. *S.D.N.Y. I Decision,* 405 F. Supp. 2d at 440 n.3. Under this reading, however, the use of the words "shall not" would prohibit a carrier even from having the *capability* to provide the government with access to information that discloses the physical location of a subscriber, regardless of whether it ever disclosed any such information to the government. Accordingly, this interpretation makes little sense and the Court declines to adopt it.

40 Notably, this phrase is "so unusual that the only time it appears in the United States Code is in [Section] 1002(a)(2)." *S.D.N.Y. I Decision,* 405 F. Supp. 2d at 442.

41 *S.D.N.Y. I Decision,* 405 F. Supp. 2d at 442.

42 The D.C. Circuit reached this same conclusion in the *United States Telecom Association* case, upholding the Federal Communications Commission's conclusion that Section 1002 "simply imposes upon law enforcement an authorization requirement different from that minimally necessary for the use of pen registers and trap and trace devices." 227 F.3d at 463; *see also Texas District Decision,* 433 F. Supp. 2d 804, slip op. at 4-5; *S.D.N.Y. I Decision,* 405 F. Supp. 2d at 441-43.

Amicus contends that the "meaning of the 'solely pursuant' language is closer to the meaning of 'pursuant.'" [43] in which case the disclosure of cell site information under the Pen Register Statute would be foreclosed, regardless of the existence of some additional statutory authority. The legislative history seems to support this view. Indeed, both the Senate and House Reports on CALEA asserted that the respective bills "expressly provide[] that the authorization under the pen register and trap and trace orders cannot be used to [*458] obtain tracking or location information, other than that which can be determined from the phone number." [44] Both reports note also that "[c]all identifying information obtained pursuant to pen register and trap and trace orders may not include information disclosing the physical location of the subscriber sending or receiving the message, except to the extent that location is indicated by the phone number." [45]

43 *Amicus* Br. 16.

44 S. REP. NO. 103-402 at 18 (1994), *available at* 1994 WL 562252; H. REP. NO. 103-827(I) at 17 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497.

45 S. REP. NO. 103-402 at 22; H. REP. NO. 103-827(I) at 22.

This interpretation, however, requires reading the word "solely" out of the statute entirely, which would violate "the settled rule that the Court must, if possible, construe a statute to give every word some operative effect." [46] Further, amicus's proposed reading would prevent the government from obtaining cell site information by *any* means because, as discussed above, any device that captures signaling information (which includes cell site information) transmitted by a cell phone is a pen register or a trap and trace device under the Pen Register Statute, [47] and these devices may be installed only pursuant to the Pen Register Statute. [48] If Congress intended, in the final analysis, to prevent the disclosure of cell site information under the Pen Register Statute even in the presence of additional statutory authority -- or to prohibit the disclosure of cell site information altogether--it could have said so explicitly. Absent any such expression in the statutory text, the Court declines to ignore the word "solely" and its implications in the context of Section 1002.

46 *E.g., Cooper Indus., Inc. v. Aviall Servs., Inc.*, 543 U.S. 157, 158, 125 S. Ct. 577, 160 L. Ed. 2d 548 (2004).

47 *See* 18 U.S.C. §§ 3127(3), (4).

48 *See* 18 U.S.C. § 3121(a); *see also S.D.N.Y. I Decision*, 405 F. Supp. 2d at 441.

Accordingly, the Court reads Section 1002 to authorize the provision of cell site information under the Pen Register Statute in combination with some unspecified, additional statutory provision. This conclusion arguably is in tension with some of the legislative history discussed above. But it appears to be the only possible choice, given the language of Section 1002. [49]

49 *See S.D.N.Y. I Decision*, 405 F. Supp. 2d at 443-44.

3. The Stored Communications Act

Finally, the government argues that Section 2703 of the Stored Communications Act provides the additional authority required by CALEA.

Section 2703(c) provides that "a governmental entity 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)" by, among means, obtaining a court order pursuant to Section 2703(d). Section 2703(d), in turn provides that any court of competent jurisdiction may issue such an order provided that the government "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."

In order to determine whether Section 2703 provides the necessary additional [*459] authority for the disclosure of prospective cell site information, the Court first must determine whether a cell phone service provider is a "provider of electronic communication service." According to the 18 U.S.C. § 2711(1), we must turn to 18 U.S.C. § 2510 for the definitions of terms used in the Stored Communications Act. Section 2510(15) defines "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Cell phone service providers clearly fit within this definition.

The next question is whether prospective cell site information is "a record or other information pertaining to a subscriber to or customer of" an electronic communications service. A number of the magistrate judges to address this question have held that Section 2703, although it might cover historical cell site data, does not authorize the disclosure of such data on a "real-time" or forward-looking basis. They assert that

> "[a]s implied by its full title ('Stored Wire and Electronic Communications and Transactional Records Access'), the entire focus of the [Stored Communications Act] is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers. Nothing in the [Stored Communications Act] contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities." [50]

This argument relies also on the lack of several procedural safeguards in the Stored Communications Act that appear in other statutes authorizing real-time, ongoing surveillance. Specifically, the magistrate judge opinions focus on the fact that the Stored Communications Act, unlike the Wiretap Act and the Pen Register Statute, does not limit the duration of law enforcement surveillance pursuant to a court order or require automatic sealing of such

orders to maintain secrecy surrounding ongoing surveillance. Several of the magistrate judges and *amicus* here contend that if Congress had intended the Stored Communications Act to permit prospective surveillance, "it would have included the same prospective features it built into the wiretap and pen/trap statutes." [51]

50 *Texas Magistrate Decision,* 396 F. Supp. 2d at 760; *see also E.D.N.Y. Decision,* 396 F. Supp. 2d at 313; *Maryland II Decision,* 416 F. Supp. 2d at 395 n.7; *Amicus* Br. 22.

51 *Texas Magistrate Decision,* 396 F. Supp. 2d at 760-61; *Amicus* Br. 22; *see also W.D.N.Y. Decision,* 415 F. Supp. 2d at 214-15;

This argument is unpersuasive. The Stored Communications Act contains no explicit limitation on the disclosure of prospective data. Further, the information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials. [52] Nor does the lack of procedural safeguards like those embodied in other surveillance statutes lend much force to amicus's position. The premise of the government's argument is that the Stored Communications Act will be used in *combination with* the Pen Register Statute, which, as noted, has procedural safeguards that the Stored Communications Act lacks. The Stored Communications Act is being asked to play only the supporting role of providing the required additional authorization for the disclosure of information already permitted by the Pen Register Statute. Accordingly, it makes sense that [*460] the Pen Register Statute would provide the procedural framework.

52 *See S.D.N.Y. I Decision,* 405 F. Supp. 2d at 446-47.

It has been argued also that Section 2703 does not authorize the disclosure of cell site information because of the definition of the term "electronic communication." Under Section 2510 (12), applicable to the Stored Communications Act by virtue of Section 2711(1), an "electronic communication"

> "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, *but does not include . . . any communication from a tracking device* (as defined in [18 U.S.C. § 3117])." [53]

Section 3117, in turn, defines "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." [54] Many of the magistrate judge opinions have concluded that (1) a cell phone is a tracking device under Section 3117 because cell site information permits the tracking of the movement of the cell phone's user, (2) cell site information is not included in the definition of "electronic communication" and (3) the disclosure of cell site information therefore is not permitted under Section 2703(c).

53 18 U.S.C. § 2510(12) (emphasis added).

54 18 U.S.C. 3117(b).

This argument also is unpersuasive. Whether a cell phone is a tracking device under Section 3117 is immaterial to the precise question before the Court, which is whether the government is entitled to an order under Section 2703. That Section, so far as is relevant here, authorizes a court, upon a proper showing, to order disclosure of "a record or other information pertaining to a subscriber to or a customer of an *electronic communications service.*" It does not authorize the disclosure of an *"electronic communication."* Further, Section 2510 does not define the scope of the term "information" under Section 2703(c) and certainly does not exclude communications from a tracking device from that term. For the tracking device exception to have force here, the Court would have to incorporate the term "electronic communication" into the term "electronic communications service." The Court declines to do because the term "electronic communications service" has its own, independent meaning under Section 2510. [55]

55 Further, incorporating the definition of "electronic communication" into the definition of "electronic communications service" has far-reaching and apparently unintended consequences. Under Section 2510(12), the term "electronic communications" excludes *any* communication from a tracking device, not just those communications that permit tracking. Therefore, if a cell phone is a tracking device by virtue of the fact that it provides cell site information, then *all* information provided by a cell phone to a cell phone service provider -- not just cell site information -- would fall outside of the scope of "electronic communication." This would mean that telecommunications service providers would not become "electronic communications service" merely by providing customers the ability to transmit information via cell phones. And if a telecommunications carrier is not an "electronic communications service," it would have no obligation to disclose *any* information to the government under Section 2703(c). Accordingly, this reading virtually eviscerates Section 2703(c).

Accordingly, because a cell phone provider is an "electronic communications service" and cell site information is a "record or other information pertaining to a subscriber to or a customer of" the cell phone provider, the logical conclusion is that Sections 2703 (c) and (d) permit a court to order the disclosure of prospective [*461] cell site information upon a proper showing by the government. The Stored Communications Act, then, provides the additional authority for cell site information required by CALEA.

* * *

Amicus argues, however, that even if the Stored Communications Act and the Pen Register Statute each authorizes the disclosure of cell site information, there is no justification for *combining* the two in the manner that the government proposes. It focuses on the fact that neither the Pen Register Statute nor CALEA mentions the Stored Communications Act

at all, and they certainly do not provide any direct authorization for the combination of authority the government proposes. While this is somewhat troubling, it is not fatal to the government's application. As noted above, CALEA's "solely pursuant" language contemplates a combination of the Pen Register Statute with some other provision and does not specifically preclude any specific statutory provision from filling that role. As the government points out, Congress passed both the Stored Communications Act and the Pen Register Statute in 1986 as part of the Electronic Communications Privacy Act and amended both with CALEA in 1994. [56] Given the two provisions' interconnected histories, it does not seem unreasonable to use them in conjunction now.

56 Gov. Rep. Br. 4-5; *see* Pub. L. No. 99-508 (1986); Pub. L. No. 103-414 (1994).

Accordingly, the Court accepts the government's argument that the Pen Register Statute and the Stored Communications Act, combined pursuant to CALEA, permit a court to authorize the disclosure of prospective cell site information, at least where, as here, the government does not seek triangulation information or location information other than that transmitted at the beginning and end of particular calls.

B. Section 3117 and the Fourth Amendment

The analysis cannot end here, however. *Amicus* and the magistrate judge opinions raise two additional issues that the Court must address.

First, some of the magistrate judge opinions suggest that because cell site information renders a cell phone a "tracking device" under 18 U.S.C. § 3117, cell site information may be disclosed only pursuant to a warrant obtained by a showing of probable cause. [57] Even assuming *arguendo* that a cell phone is a tracking device under Section 3117, this argument is unavailing.

57 *Texas Magistrate Decision*, 396 F. Supp. 2d at 757-58; *E.D.N.Y. Decision*, 396 F. Supp. 2d at 323.

First, Section 3117 provides that "[i]f a court is empowered to issue a warrant or *other order* for the installation of a mobile tracking device, 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." [58] Accordingly, Section 3117 specifically "contemplates that a tracking device may be installed pursuant to an 'order' -- that is, without a warrant and thus without a probable cause showing." [59]

58 Emphasis added.

59 *S.D.N.Y. I Decision*, 405 F. Supp. 2d at 449 n.8.

Further, Section 3117 speaks only to the "installation" of a tracking device. Here, the government does not seek to *install* any sort of tracking device, as cell phones provide location information on their own by transmitting signals to nearby antenna towers.

[*462] *Amicus* next argues that permitting the disclosure of cell site information under the Pen Register Statute and the Stored Communications Act would violate the Fourth Amendment prohibition on unreasonable searches and seizures. It contends that granting this application would permit the government to track the location of the target cell phone -- and its user -- without a warrant and a showing of probable cause. This, it says, would run afoul of *United States v. Karo,* [60] which held that the government may not install a tracking device without the knowledge of the person being tracked or a warrant if the device would disclose its location inside a person's home and that information could not have been observed from public spaces.

60 468 U.S. 705, 714, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984).

The government argues that there is no Fourth Amendment problem because cell phone users have no legitimate privacy interest in information they voluntarily turn over to third parties. It relies chiefly on *Smith vs. Maryland,* [61] in which the Supreme Court held that there is no legitimate privacy interest in telephone numbers dialed because telephone users voluntarily convey those numbers to the telephone company in order to place calls, thereby assuming the risk that the telephone company will pass that information on to law enforcement officials.

61 442 U.S. 735, 742-44, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979).

The Court cannot resolve the Fourth Amendment question in the abstract. Although the government is correct that, under *Smith,* there is no legitimate expectation of privacy in the telephone numbers dialed from a particular telephone, it does not necessarily follow that a cell user abandons any legitimate expectation of privacy in his or her *location* by carrying a cell phone that signals its presence in the network to the service provider. Assuming *arguendo* that a cell phone user maintains at least some expectation of privacy in location, the government could violate *Karo* if it used cell site information to surveil a target in a private home that could not be observed from public spaces. At this point, however, the Court has no way of knowing if the government will use any cell site information it obtains in this manner. If it does, and information obtained leads to indictment, the issue can be litigated on a motion to suppress.

E. Application

Having concluded that it can order the disclosure of prospective cell site information pursuant to the combined authority of the Pen Register Statute and the Stored Communications Act, the Court must determine whether the government's application meets the requirements under those statutes. As discussed above, the Pen Register Statute authorizes a court to order the installation and use of a pen register or a trap and trace device upon an application by the government certifying that "information likely to be obtained from such installation and use is relevant to an ongoing criminal investigation." [62] The Stored Communications Act permits a court order where 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." [63] The government's sealed application, which the Court has reviewed *in camera,* meets both of these requirements.

62 18 U.S.C. § 3123.

63 18. U.S.C. § 2703(d).

[*463]

Conclusion

For foregoing reasons, the government's application for an order authorizing the use of a pen register with a trap and trace device is granted. The pen register and/or trap and trace device is authorized to capture (1) the calls made and received by the subject cell phone and (2) information which identifies the antenna tower receiving transmissions from that cell phone at the beginning and end of a particular telephone call made or received by the telephone's user, including any information on what portion of that tower is receiving a transmission at the beginning and end of a particular telephone call.

SO ORDERED.

Dated: October 23, 2006

Lewis A. Kaplan

United States District Judge