October 27, 2005

BY HAND

Honorable Andrew J. Peck
Chief United States Magistrate Judge
Southern District of New York
United States Courthouse
500 Pearl Street, Room 750
New York, New York 10007

Re: In re Government Application for Pen Register and Trap and Trace Device with Cell-Site Location Authority

Dear Chief Magistrate Judge Peck:

The Federal Defenders of New York, Inc. ("FDNY"), is a Community Defender Organization organized under 18 U.S.C. § 3006A and operates pursuant to the CJA plans for the United States District Courts for the Southern and Eastern Districts of New York as the federal public defender office for these Districts. At the suggestion of Magistrate Judge Gorenstein, we submit this letter brief as amicus curiae in connection with the Government's pending application seeking an order from the Court to obtain "cell-site location" data based on 18 U.S.C. § 2701 et seq., the Stored Communications Act ("SCA"), and 18 U.S.C. § 3121 et seq., the Pen Register / Trap-Trace Statute ("Pen/Trap Statute").[1] The Government has submitted a letter brief in support of its application. See Letter of AUSA Thomas G.A. Brown, October 5, 2005 ("Gov. Br.").

---

[1] Statement of Interest of *Amicus*: As the Community Defender Organization for this District as well as the Eastern District of New York, the FDNY represents, and is likely to represent in the future, persons who are or may become a target of a Government investigation in which the Government seeks to obtain information regarding that individual's cell phone usage, including cell-site data. The legal issue raised in the instant application -- whether the Government can obtain cell-site data based on a combination of the SCA and the Pen/Trap Statute -- thus has ramifications for FDNY's current and future clients.

Only two courts have directly addressed this question, and both rejected the Government's application for cell-site date based on the same statutes it relies on before this Court. See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, ___ F. Supp.2d ___, 2005 WL 2656621 (S.D. Tx. Oct. 14, 2005) ("Texas Op."); In re Application of the United States for an Order Authorizing Use of Pen Register and Trap / Trace Device and Authorizing Release of Subscriber Information and/or Cell Site Information, ___ F. Supp.2d ____, 2005 WL 2739208 (E.D.N.Y. Oct. 24, 2005) ("EDNY Op.").[2]

Amicus submits that these decisions are correct: Neither the SCA nor the Pen/Trap Statute, either individually or in combination, authorizes the issuance of an order permitting the Government to obtain cell-site data that would allow it to locate and track a person's whereabouts through his or her cell phone. Rather, a search warrant issued pursuant to Fed. R. Crim. P. 41,

---

[2] A copy of the Texas Opinion is attached as Exhibit A and a copy of the EDNY Opinion is attached as Exhibit B. Each is presented in its original slip opinion form, and this letter brief will refer to those Opinions by the page numbers indicated in that format.

The EDNY Opinion was issued on the Government's motion for reconsideration of an earlier decision. See In re Application of the United States for an Order Authorizing Use of Pen Register and Trap / Trace Device and Authorizing Release of Subscriber Information and/or Cell Site Information, 384 F. Supp.2d 562 (E.D.N.Y. Aug. 25, 2005). The new decision substantially revises the earlier one, but largely follows the reasoning and result of Magistrate Judge Smith's Texas Opinion.

issued only upon a showing of probable cause, must be obtained before such information can be gathered by the Government. The Court should reject the Government's attempt to end-run the probable cause requirement of Rule 41 and the Fourth Amendment.

STATEMENT OF FACTS

1. Cell Phones and Cell-Site Data Basics

A cellular telephone, or cell phone, "is a sophisticated two-way radio with a low-power transmitter that operates in a network of cell sites." Texas Op. 3. That network functions "by dividing a geographic area into many coverage areas, or 'cells,' each containing a tower through which an individual portable cell phone transmits and receives calls." Gov. Br. 1.

When a cell phone is turned on, "it acts as a scanning radio" that constantly searches for the strongest available signal, usually emanating from the cell tower closest to it within the network. Texas Op. 4. To ensure the best reception at all times, the cell phone automatically "re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed" or received by the phone. Id. (emphasis added); see Note, Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 Harv. J.L. & Tech. 307, 308 (2004) (hereinafter "Note") ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register."). At any given time, therefore, a cell phone provider is aware of the particular cell tower within its network to which a specific cell phone is directing (or receiving) a signal. Gov. Br. 1.

Even more, the provider is aware of the specific "portion of the tower facing" the cell phone -- i.e., the precise angle or direction from which the cell phone is transmitting its signal to (or receiving a signal from) a particular tower. Id. "[T]he [cell] tower records the angle at which a phone's signal arrives at the station." Note, supra, at 309.

Additionally, a cell phone provider is able to discern the distance between the cell phone and the particular cell tower to which it is registered. When a cell phone connects to (i.e.,

"registers" with) a particular cell tower, "the tower measures the amount of time it takes for the signal to leave one location and reach the other." Note, supra, at 308. Where the cell phone initiates the contact, for instance, "the tower measures the time it takes the signal to get from the phone to the tower." Id. at 308-309. Similar timing information can be derived when the cell provider initiates a signal that travels from the tower to the cell phone. Id. at 309.

Using this host of cell-site data, a cell phone provider can pinpoint the location of a particular cell phone within a cell, as well as track its movements between cells within the entire network. Combining the information concerning the particular angle at which a cell phone is facing a specific cell tower with the "timing" information concerning the distance that the phone is from that same tower, for instance, a provider can pinpoint the phone's physical location as well as track its movements. Note, supra, at 309.

Even without timing information, a cell provider can readily discern the location of a cell phone whenever -- as is frequently the case -- it transmits signals to (or receives signals from) more than one cell tower. "When multiple towers receive signals, the system can compare the angles of arrival and thus triangulate the relative location of the cell phone." Note, supra, at 309. Such "signal triangulation" is especially effective in urban areas, where the "number of towers and their sectioning into directional 'faces' (north face, south face, etc.) gives providers access to quite accurate location information." Id.

Cell-site data, in sum, allows a cell provider to "creat[e] a virtual map of [a cell phone user's] movements" so long as the user does not turn off his or her phone, regardless of whether he or she initiates or receives a call. Note, supra, at 309. By the triangulation process, for instance, "law enforcement is able to track the movements of [a] target phone, and hence locate a suspect using that phone." Texas Op. 5. Popular press accounts are replete with examples of such feats by law enforcement. See generally Note, supra, at 310-311 (discussing several well-publicized incidents of police locating a kidnaping victim or a suspect by using cell-site data).

2. The Government's Application for Cell-Site Location

Information

The Government seeks an order from this Court that, inter alia, would allow it to obtain "cell-site location information" for the target cell phone. See Gov. Br., Exh. A at 2.[3] As it acknowledges, such information "conveys data concerning the particular location of a cell phone and its user," Gov. Br. 5, and will be "used by [G]overnment agents to, among other things, help locate kidnaping victims and fugitives or other targets of criminal investigation," id. at 2.

[3] This letter brief does not address any aspect of the Government's application other than its request for cell-site data.

The Government relies on two statutes, the Pen/Trap Statute, 18 U.S.C. § 3121 et seq., and the SCA, 18 U.S.C. § 2701 et seq., in its application. Specifically, the Government contends that § 2703(d) of the SCA, in combination with a pen register device issued pursuant to § 3123, authorizes the disclosure, on both a prospective and a retrospective basis, of cell-site data for the target cell phone based merely on a demonstration by the Government of "'specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records of other information sought are relevant and material to an ongoing criminal investigation.'" Gov. Br. 2, quoting 18 U.S.C. § 2703(d).[4]

These are the same authorities it presented to Magistrate Judge Orenstein in the Eastern District of New York and Magistrate Judge Smith in the Southern District of Texas in support of applications for the same cell-site data that it seeks here. As indicated, both courts rejected the Government's application.

ARGUMENT

Point I

THE SCA DOES NOT AUTHORIZE DISCLOSURE OF CELL-SITE DATA

The Government contends that "existing" cell-site data, possessed by a cell phone provider for the target cell phone, can be obtained under the Stored Communications Act ("SCA"), and specifically via 18 U.S.C. § 2703(c) & (d). Gov. Br. 4. It claims that "cell-site information constitutes 'information

[4] Whether the Government has made such a showing in this particular case is not addressed by amicus. This letter brief proceeds on the assumption the Government has satisfied § 2703(d)'s standard, and argues simply that neither § 2703(d) nor the Pen/Trap Statute, nor the two in combination, authorizes disclosure of cell-site data even when that standard has been met.

pertaining to a subscriber'" within the meaning of § 2703(c), and thus disclosable to the Government upon a showing under § 2703(d) of "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records of other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The Government is wrong. Cell-site data is not encompassed within § 2703 because it constitutes information derived from a "communication from a tracking device (as defined in section 3117 [of Title 18]," and thus specifically excluded from disclosure under the SCA pursuant to 18 U.S.C. § 2510(12)(C). In any event, even if cell-site data falls within § 2703(c)'s category of "information pertaining to a subscriber," the SCA does not authorize the prospective disclosure of cell-site data, which the Government seeks in its application. At best, the Government may obtain only historic information under the SCA, not the prospective and on-going data it desires.

1. Cell-Site Data Constitutes "Communication from a Tracking Device," Which Is Specifically Excluded from the SCA's Reach.

The SCA can be found from § 2701 to § 2712 of Title 18 of the United States Code. Section 2703 is its core, and states in relevant part:

> (c) **Records concerning electronic communication service . . . --**
>
> (1) A government 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 communication) only when the governmental entity --
>
> (A) obtains a warrant . . . ;
> (B) obtains a court order for such disclosure under subsection (d) of this section;
> . . .

> (d) **Requirements for court order –** A court order for disclosure under subsection . . . (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. §§ 2703(c) & (d) (bold in original). As noted, the Government contends that cell-site data falls within the category of "information pertaining to a subscriber," id. § 2703(c), and thus must be disclosed to the Government pursuant to § 2703(c)(1) upon issuance of an order by the Court under § 2703(d). See Gov. Br. 4.

The Government misreads § 2703(c). More precisely, it reads only half of § 2703(c). Read in its entirety, § 2703 does not authorize the disclosure of cell-site data.[5]

The critical phrase "information pertaining to a subscriber" is nowhere defined. See 18 U.S.C. § 2511 (setting forth definitions for the SCA). But whatever this phrase encompasses, it is explicitly qualified by the terms "electronic communication" or "electronic communication service," which appear twice in § 2703(c). Read in context, the subscriber-related information that the Government seeks is limited to either (1) subscriber-related information pertaining to an "electronic communication," or (2)

---

[5] The Government apparently assumes that information falls only in two categories -- content and non-content. If it is content, then it is governed by § 2703(a) & (b). And if it is non-content, it is governed by § 2703(c). All non-content information, the Government assumes, is encompassed by § 2703(c), and thus disclosable pursuant to an order issued under § 2703(d). See Gov. Br. 5-6.

There is no basis for this assumption. Rather, as a careful reading of § 2703(c) reveals, see infra, this provision covers only information derived from or pertaining to an "electronic communication." Information specifically excluded from the definition of "electronic communication" cannot therefore be disclosed under § 2703(c), even if it is "non-content."

subscriber-related information kept by an "electronic communication service." The very title to § 2703(c) -- "Records concerning electronic communication service . . . " (emphasis added) -- proves this interpretation.

Fortunately, these two terms are defined. Section 2711(1) of the SCA explicitly incorporates the definitions given in § 2510, among which is "electronic communication service" and "electronic communication."

To begin, "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). This definition is not helpful, since it circularly refers to the term "electronic communication."[6]

The statute also defines "electronic communication," however, and this definition is enlightening:

> (12) "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 --
>
> . . .
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); . . . .

18 U.S.C. § 2510(12) (emphasis added). "By virtue of this tracking device exclusion," therefore, "no communication from a tracking device" qualifies as an "electronic communication."

---

[6] Clearly, a "wire communication" is not at issue here, since such communication must involve a transfer of the human voice, see 18 U.S.C. §§ 2501(1) & (18), and the Government does not seek to obtain such information. See United States v. Forest, 355 F.3d 942, 949 (6th Cir. 2004) ("Cell-site data clearly does not fall within the definitions of wire or oral communication . . . .").

Texas Op. 19.

A fortiori, subscriber-related information pertaining to an "electronic communication," or subscriber-related information kept by an "electronic communication service," id. § 2703(c), does not include information derived from "[a]ny communication from a [§ 3117] tracking device." If "[r]eal-time location monitoring [via cell-site data] effectively coverts a cell phone into a tracking device," therefore, such information would not qualify as "electronic communication" under § 2510(12)(C) and thus cannot be sought under the authority of § 2703(c) & (d). Texas Op. 19.

Section 3117 confirms that the Government's use of cell-site data to locate a person and track his or her movements converts a cell phone into a tracking device within the meaning of that section. As § 3117(b) defines, "the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).

The definition "is striking for its breadth." Texas Op. 9. As Magistrate Judge Smith pointed out,

> a device is covered [by § 3117(b)] even though it may not have been intended or designed to track movement; it is enough if the device merely "permits" tracking. Nor does the definition suggest that a covered device can have no function other than tracking movement. Finally, there is no specification of how precise the tracking must be. Whether from room to room, house to house, neighborhood to neighborhood, or city to city, this unqualified definition draws no distinction.

Id. 9-10.

A cell phone is not designed as a tracking device, nor is that its primary function. Nonetheless, when the Government uses cell-site data from a cell phone to "locate kidnaping victims and fugitives or other targets of criminal investigations" by means of the signals sent by the cell phone to cell towers, Gov. Br. 2, it unquestionably employs that phone as "an electronic . . . device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).

The Department of Justice itself uses an electronic device known as a "trigger-fish," which "enables law enforcement to gather cell-site data directly, without the assistance of the service provider," to track the location and movements of a target. Texas Op. 12-13. The trigger-fish "identifies the location of the user by exactly the same triangulation method that the [G]overnment would apply to cell site data obtained from the cell phone company." Id. at 13. And the DOJ repeatedly describes this device as a "tracking device":

> In order to use such a device the investigator generally must known the target phone's telephone number . . . . After the operator enters the information into the tracking device, it scans the surrounding airwaves. When the user of that phone places or receives a call, the phone transmits its unique identifying information to the provider's local cell tower. The provider's system then automatically assigns the phone a particular frequency and transmits other information that will allow the phone properly to transmit the user's voice to the cell tower. By gathering this information, the tracking device determines which call . . . on which to home in. When the user remains on the phone, the tracking device can then register the direction and signal strength (and therefore the approximate distance) of the target phone.

U.S. Dep't of Justice, Electronic Surveillance Manual 44-45 (rev. June 2005) (emphases added), quoted in Texas Op. 13 n.12.[7]

---

[7] United States v. Forest, 355 F.3d 942 (6th Cir. 2004), additionally illustrates the Government's use of a cell phone as a tracking device. While following two suspects under investigation for narcotics trafficking, DEA agents lost visual contact of their vehicle. The agents then used the cell phone of one suspect to track his movements:

> In order to reestablish visual contact, a DEA agent dialed Garner's cellular phone (without allowing it to ring) several times that day and used Sprint's computer data to determine which transmission towers were being "hit" by Garner's phone. This "cell-site data" revealed the general location of Garner.

What's good for the goose is good for the gander: "If the tracking device label is warranted in one case, it is warranted in the other." Texas Op. 13. Using cell-site data from a cell phone provider to track a target phone's movements constitutes using that cell phone as a tracking device. Cell-site data used to track a target's location and movement via signals from his cell phone, therefore, constitutes a "communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510(12)(c).

From this data DEA agents determined that Garner had traveled to the Cleveland area and then returned to the area of Youngstown / Warren.

Id. at 947. As Magistrate Judge Smith noted, "Garner's cell phone functioned no differently than a traditional beeper device, the only difference being that it was on his person instead of attached to his vehicle." Texas Op. 11.

As such, cell-site data does not qualify as an "electronic communication." Id. In turn, cell-site data does not constitute either (1) subscriber-related information pertaining to an "electronic communication," or (2) subscriber-related information kept by an "electronic communication service" within the meaning of § 2703(c). Disclosure of cell-site data is therefore not authorized by an order issued pursuant to § 2703(d).[8]

2. Even if the SCA Allowed Disclosure of Cell-Site Data, It Does Not Authorize Prospective or On-Going Gathering of Such Information.

Even if the SCA authorized disclosure of cell-site data upon satisfaction of the § 2703(d) standard, it would only authorize disclosure of historic or "existing" data already possessed by the provider, Gov. Br. 4, and would not allow the Government to obtain such data on a prospective or on-going basis, as it seeks in the instant application. See generally EDNY Op. 31-33. The full title of the SCA itself confirms this -- it is the "Stored Wire and Electronic Communications and Transactional Records Access Act." (emphasis added). And "[i]t is well established that the title of a statute or section is an indication of its meaning." Bell v. Reno, 218 F.3d 86, 91 (2d Cir. 2000).

---

[8] As discussed below, this result makes perfect sense because, as a general matter, the Government must obtain a search warrant issued upon a showing of probable cause before it can use a beeper or tracking device to trace a person's movements. See infra Point IV. A § 2703(d) order, in contrast, can be issued upon a lesser showing akin to the reasonable suspicion standard – i.e., whenever the Government offers "specific and articulable facts" showing "reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

"[T]he entire focus of the SCA is to describe the circumstances under which the [G]overnment can compel disclosure of existing communications and transaction records in the hands of third party service providers. Nothing in the SCA contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities." Texas Op. 20-21 (emphasis added). The Department of Justice agrees: "Any real-time interception of electronically transmitted data in the United States must comply strictly with the requirements of Title III, 18 U.S.C. §§ 2510-2522 [The Wiretap Act], or the Pen/Trap Statute, 18 U.S.C. §§ 3121-3127," while "18 U.S.C. §§ 2701-12 [The SCA] . . . governs how investigators can obtained stored account records and contents . . . ." U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations ix, 24 (July 2002), available at http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf (emphases added). Academic commentators concur that a significant distinction exists between retrospective and prospective surveillance, and that surveillance under the SCA is solely retrospective. See, e.g., Deirdre Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1565 (2004); Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 Ala. L. Rev. 9, 46-52 (2004). Cf. Orin S. Kerr, Internet Surveillance Law after the USA PATRIOT Act: The Big Brother that Isn't, 2003 Nw. U. L. Rev. 607, 616-18 (2003) (noting difference between prospective and retrospective surveillance).

The structure and content of the SCA confirm that it is targeted solely to historic data and does not authorize the gathering of data on an on-going or prospective basis. See Texas Op. 21-22; EDNY Op. 24-25. Unlike the Wiretap Act or the Pen/Trap Statute, both of which are unquestionably prospective in nature, the SCA contains no durational limit for § 2703(d) orders. Compare 18 U.S.C. § 2518(5) (wiretap authorization limited to 30 days), and id. § 3123(c)(1) (pen/trap authorization limited to 60 days). Moreover, there is no provision in the SCA requiring the service provider to provide the technical assistance necessary for prospective surveillance -- unlike the Wiretap Act and the Pen/Trap Statute. Compare 18 U.S.C. § 2511(2)(a)(ii) (directing

phone company to assist with implementing wiretap), and id. § 3123(b)(2) (directing phone company to furnish "technical assistance necessary to accomplish the installation of the pen register or trap and trace device"). An order issued pursuant to § 2703(d) only commands the service provider to "disclos[e]" the materials sought, and nothing more. See EDNY Op. 33-34.

In sum, § 2703(d) merely "permits access to customer transaction records currently in the hands of the service provider, relating to the customer's past and present use of the services. . . . [It] contemplates the production of existing records, not documents that may be created at some future date related to some future communication." Texas Op. 22. The Government's request for an order commanding the cell phone provider "to capture and report at the same time originating and terminating cell site location information," Gov. Br. Exh. A at 1-2, "for a period of sixty days from the date of th[e] [requested] order" id. at 6, therefore, is simply not encompassed within the SCA.

Point II

THE PEN/TRAP STATUTE DOES NOT AUTHORIZE THE CAPTURE OF CELL-SITE LOCATION DATA

The Pen/Trap Statute, 18 U.S.C. § 3121 et seq., unquestionably authorizes surveillance on an on-going and prospective basis. However, it does not allow the Government to obtain cell-site location data. This is so for two reasons.

First, by definition, the Government cannot obtain cell-site data via a pen register or a trap-and-trace device, which are limited to gathering basic information concerning the origin, destination, direction, and duration of a call. The Government's reliance on the newly expanded definitions for these devices, enacted pursuant to the USA PATRIOT Act of 2001 ("PATRIOT Act"), is misplaced. Those amendments were directed solely toward ensuring that pen/trap devices could be used to gather Internet-generated data, and had nothing to do with cell phones generally or cell-site data specifically.

Second, Section 103(a)(2) of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), codified at 42 U.S.C. §

1002(a)(2)(B), specifically excludes "any information that may disclose the physical location of the subscriber" from the type of information that may be gathered by a pen/trap device. Because cell-site data qualifies as "information that may disclose the physical location of the subscriber," as even the Government concedes, Gov. Br. 9, such data may not be obtained via a pen/trap device.

1. Pen Registers and Trap/Trace Devices, by Definition, Cannot Be Used to Gather Cell-Site Data.

Historically, a pen register is a device that captures the phone number dialed by a target telephone while making an outgoing call, and a trap-and-trace device is a mechanism that captures the phone number of an incoming call to a target telephone. See Kerr, supra, at 632-33. Prior to the PATRIOT Act's amendment of the federal Pen/Trap Statute, § 3127 conformed with this traditional understanding:

> (3) the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached . . . ;
>
> (4) the term "trap and trace device" means a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;

18 U.S.C. § 3127 (2000 edition).

Before 2001, "the definitions of the terms 'pen register' and 'trace and trace device' did not make clear whether they applied only to the telephone, or whether they could also apply to the Internet." Kerr, supra, at 633. The pen register's reference to "the numbers dialed . . . on the telephone line" seemed to indicate that it did not encompass Internet transmissions, such as e-mails. And while the trap/trace definition was somewhat broader, it too referred solely to information "identify[ing] the originating number" of the originating "instrument or device".

No published decision confronted this issue. And the only known unpublished decisions came to opposing conclusions: While a Magistrate Judge in Los Angeles ruled that pen/trap devices applied to the Internet, a Magistrate Judge in the Northern District of California ruled to the contrary. See Kerr, supra, at 634-636.

The law remained uncertain until the events of September 11, 2001, which led directly to the passage of the PATRIOT Act the following month. In the PATRIOT Act, Congress "updat[ed] the pen register statute so that it clearly applied to the Internet." Kerr, supra, at 637 (emphasis added); see Freiwald, supra, at 60-61 (similarly noting that PATRIOT Act amended pen/trap definitions in order to encompass Internet data). Instead of "rewrit[ing] the entire statute, the DOJ proposed [simply] to amend the definition of 'pen register' and 'trap and trace device' to make clear that it applied broadly to network envelope information, encompassing both telephones and the Internet." Kerr, supra, at 637 (emphasis added). This proposal was adopted by Congress. Id. at 637-38.

As amended by the PATRIOT Act, § 3127 now provides:

> (3) the term "pen register" means 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 . . . ;
>
> (4) the term "trap and trace device" mans a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication . . . ;

18 U.S.C. § 3127 (2005).

The Government seizes upon these broadened definitions, arguing that cell-site data can now be captured by pen/trap devices because "cell-site information constitutes 'dialing, routing, addressing, and signaling information.'" Gov. Br. 8.

This argument must be rejected. The Court should not accept the Government's invitation to casually read into the statute what Congress never intended.

The host of cell-site information sought by the Government in its application does not constitute "dialing, routing, addressing, and signaling information." Despite the recent amendment, the essential nature of pen/trap devices has not changed: They are mechanisms or processes that enable the Government to obtain basic information about the source, destination, direction, and duration of a transmission, be it telephonic or electronic. Cell-site data falls into an altogether different category -- detailed information concerning which cell tower the target phone is registered to, the angle at which the phone's signal approaches that tower, and the time in which a signal travels from the phone to the tower. Allowing the Government to track an individual's movements through a pen/trap device would constitute an unprecedented expansion of the device's reach.

Traditionally, moreover, a pen/trap device "was triggered only when the user dialed a telephone number" or received a phone call. Texas Op. 24-25. "[N]o information was recorded by the device unless the user attempted to make a call" or received an incoming call. Id. at 25. And while the PATRIOT Act expanded the definition of such devices, it continued to insist that the "routing, addressing, and signaling" information "is generated by, and incidental to, the transmission of a 'wire or electronic communication.'" Id., quoting 18 U.S.C. § 3127(3). "In other words, today's pen register must still be tied to an actual or attempted phone call." Id.

In contrast, cell-site data can be captured regardless of whether a call is made by or made to the target cell phone. E.g., Note, supra, at 308 ("Even when users are not making or receiving calls, cell phones communicate with the nearest cell tower to register."). That is, cell-site data is captured even when no wire or electronic communication is "transmitted" within the meaning of § 3127(3). Such data, therefore, is not the kind of information that can be captured or disclosed by a pen/trap device.

In any event, the Government's construction succeeds only by untethering the definitions from their original, Internet-derived moorings. As discussed above, the PATRIOT Act's amendment to the Pen/Trap Statute had nothing to do with cell phones. Rather, the amendment was proposed and adopted to clarify that pen/trap devices applied not only to telephonic transmissions but also Internet transmissions. See Kerr, supra, at 633-38.

"Nothing in the . . . legislative history of the PATRIOT Act suggests that this new definition would extend the reach of the Pen/Trap statute to cell phone tracking." Texas Op. 24. And "[c]ontemporary summaries of the PATRIOT Act prepared by knowledgeable commentators, including the DOJ itself, make no mention of expanding pen/traps to capture cell site data." Id. (emphasis added). The "PATRIOT Act's expansion of pen/trap definitions," in sum, "was intended only to reach electronic communications such as e-mail." Id.; accord EDNY Op. 41-42.

Given the unprecedented nature of the Government's attempt to use pen/trap devices to track the movements of a targeted individual, this Court must tread cautiously. At the least, it should adopt the Government's reading only if Congress unambiguously intended such a result. Because Congress did not so intend, see supra, the Government's reading must be rejected.

2. Pen/Trap Devices Cannot Be Used to Reveal the Physical Location of the Target.

Indeed, a 1994 amendment to the Pen/Trap Statute explicitly prohibits a service provider from disclosing information to the Government concerning a user's "physical location" through the use of a pen/trap device. Section 1002 of Title 42, as amended by the CALEA of 1994, now states:

> **(a) Capability requirements**
>
> . . . [A] telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of --
>
> (1) expeditiously isolating and enabling

> the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area . . . ;
>
> (2) 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 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);

47 U.S.C. § 1002 (2005) (emphasis added).

Even the Government concedes that "'information that may disclose the physical location of the subscriber' includes cell-site information of the kind" sought in its application. Gov. Br. 9. Therefore, "[t]he Government [] cannot rely upon the Pen/Trap Statute alone . . . to obtain cell-site information." Id. at 8.

Point III

NO "HYBRID" AUTHORITY JUSTIFIES DISCLOSURE OF CELL-SITE DATA PURSUANT TO A § 2703(d) ORDER

Grasping on the "solely pursuant" language of § 1002, the Government ingeniously constructs a new "hybrid" creature capable of sustaining its application for cell-site data. As it asserts:

> Under the Pen/Trap Statute, a court is empowered to authorize the installation of a pen register or trap

> and trace device upon [a] finding . . . [pursuant to] 18 U.S.C. § 3123(b). Recognizing the complementary role played by the SCA, and to comply with CALEA [i.e., 47 U.S.C. § 1002(a)], the Government also seeks cell-site authority based on an additional showing, pursuant to Section 2703(d), that the information is "relevant and material to" [an] investigation. 18 U.S.C. § 2703(d). Accordingly, the Government submits that the Court has authority to issue cell-site orders pursuant to the combined authority of the Pen/Trap Statute and Section 2703(d) of the SCA.

Gov. Br. 10. The Court should quickly reject this argument.

First and foremost, the Government's argument makes no sense given the points made in the preceding sections. As argued, neither § 2703(d) of the SCA nor § 3127 of the Pen/Trap Statute authorizes the disclosure of cell-site data. See supra Point I.1 and Point II.1 & II.2. Unless some unknown synergy is generated by their combination, it defies reason to claim that a "hybrid order" suffices to authorize the disclosure of cell-site data.

In any event, the combined § 3123(b) / § 2703(d) order proposed by the Government is a chimera in the original sense of the word: a mythical monster composed of disparate parts, a creature that does not exist in nature. It is an animal entirely of the Government's own making, found nowhere in the United States Code. The Government's argument must be rejected for this reason alone.

As Magistrate Judge Smith points out, moreover, the relevant statutes do not even cross reference or mention each other:

> The Pen/Trap Statute does not mention the SCA or CALEA; SCA § 2703 does not mention CALEA or the Pen/Trap Statute; and the CALEA proviso does not mention the SCA. CALEA does refer to the Pen/Trap Statute, but only in the negative sense of disclaiming its applicability.

Texas Op. 28.

This silence is especially meaningful given that § 2703(d) and § 1002 were both enacted as part of the 1994 CALEA. If these two provisions were so intimately intertwined, as the Government asserts, surely Congress would have made the connection explicit. No such connection -- not even the barest hint of a link -- exists, however. As Magistrate Judge Smith concluded, "Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way." Id. at 28-29.

Finally, the existence of the Government's hybrid is disproved by the lack of a discernable birthday. As noted, § 1002 and § 2703(d) were enacted in 1994 as part of CALEA. The Government's theory is that § 1002's "solely pursuant" language implicitly refers to § 2703(d), and authorizes the disclosure of cell-site data by means of a pen/trap device when such a device is used in connection with a § 2703(d) order.

However, even the Government acknowledges that a pen/trap device could not have been used to obtain cell-site data before 2001, when the PATRIOT Act amended the traditional definitions of pen/trap devices. See supra Point II.1. Therefore, the Government's hybrid could not have existed before 2001.

But this makes no sense. After all, the Government is relying on § 2703(d) and the negative pregnant of § 1002 to do the heavy lifting in its effort to obtain cell-site data. These sections, however, were born seven years before the PATRIOT Act. The Government, in short, is claiming that a 2001 statute changed the meaning of two statutory provisions enacted in 1994.[9] Of course, even the Government must concede that the PATRIOT Act says nothing about either § 2703(d) or § 1002.

As Magistrate Judge Smith concluded, "The Government's hybrid theory, while undeniably creative, amounts to little more

[9] The mystery deepens when one considers that the effective date of § 1002's "solely pursuant to" provision was "delayed for four years after [CALEA's 1994] enactment," while the other provisions of CALEA, including § 2703(d) of the SCA, "became effective immediately." EDNY Op. 44.

than a retrospective assemblage of disparate statutory parts to achieve a desired result." It must be rejected.

Point IV

A SEARCH WARRANT ISSUED UPON A SHOWING OF PROBABLE CAUSE IS REQUIRED TO OBTAIN CELL-SITE DATA

The Government claims that "[a]ny argument that the Pen/Trap Statute and Section 2703(d) cannot be combined would render the 'solely pursuant' language [of § 1002] surplusage, a result which Congress could not have intended." Gov. Br. 10. It is again mistaken.

A Rule 41 search warrant, issued upon a showing of probable cause, suffices to authorize disclosure of cell-site data in connection with an order issued under the Pen/Trap Statute. The "solely pursuant" language of § 1002 is thus not rendered surplusage.[10] This position has the additional virtue of conforming with Supreme Court law concerning tracking devices that may reveal non-public information during its use by law enforcement. See, e.g., Texas Op. 6-7 ("A Rule 41 probable cause warrant [is] the standard procedure for authorizing the installation and use of mobile tracking devices.") (citing cases).

1. A Search Warrant Is Required for a Roaming Tracking Device that May Reveal Non-Public Information.

As noted, the host of cell-site data the Government seeks would allow it to pinpoint the location of the target cell phone as well as its movements within the provider's network. Indeed, using the requested data to monitor a target cell phone

[10] Judge Orenstein similarly suggests that the "solely pursuant to" language of § 1002 would not be rendered surplusage if a wiretap order were sought in conjunction with an application for a pen/trap device to acquire cell-site data. EDNY Op. 46.

effectively converts it into a tracking device within the meaning of § 3117(b). See supra Point I.1. Given the small size of a cell phone, and given that most users carry their cell phones on their person, moreover, this tracking device will reveal the user's whereabouts and movement in a wide array of locations. Some of these locations will be public; others will be private.

The Supreme Court has permitted warrantless location tracking where the information obtained by the tracking device could have been obtained by visual surveillance from public places. United States v. Knotts, 460 U.S. 276 (1983). In Knotts, the defendant challenged the warrantless use of a beeper that the police placed in a chemical drum that the defendant later put in his car. While the police monitored the drum's movements on public roads, there was no evidence that the beeper was monitored while it was inside the defendant's house. See id. at 282 ("Visual surveillance from public places along [defendant's] route or adjoining [his] [home] would have sufficed to reveal all of these facts to the police.").

The Court thus rejected the defendant's Fourth Amendment challenge, concluding that because the beeper yielded only information that could have been obtained visually from public locations, no Fourth Amendment interest was implicated. Id. at 282-83.

The Court carefully pointed out the limited nature of its holding, however. As it explained, "nothing in this record indicates that the beeper signal was received or relied upon after it had indicated that the drug . . . had ended its automotive journey at rest on respondent's premises in rural Wisconsin." Id. at 284-85.

In a case decided the following year, the Supreme Court reached this precise question and ruled that the Fourth Amendment prohibits the warrantless use of a tracking device that revealed non-public information. In United States v. Karo, 468 U.S. 705, 714 (1984), the beeper was monitored while it was inside the defendant's home. Unlike the situation in Knotts, where "the record did not show that the beeper was monitored while the can containing it was inside the cabin," 468 U.S. at 714, "there is no gainsaying that the beeper was used [in this case] to locate the

ether in a specific house . . . ." Id. The Court seized upon this difference to rule that "the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment." Id. Use of such a beeper requires a search warrant issued upon probable cause. Id. at 715-17.

Critical for the instant matter is the Court's response to the Government's complaint that "[i]f agents are required to obtain warrants prior to monitoring a beeper when it has been withdrawn from public view, . . . for all practical purposes they will be forced to obtain warrants in every case in which they seek to use a beeper, because they have no way of knowing in advance whether the beeper will be transmitting its signals from inside premises." Id. at 718. The Court curtly dismissed this complaint:

> The 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.

Id. Implicit in this response, of course, is that the Government should obtain a search warrant "in every case in which . . . they [do not] know[] in advance whether the beeper will be transmitting its signals from inside premises." See also id. at 713 n.3 (given that law enforcement cannot know when a beeper has been withdrawn from public view, "warrants for the installation and monitoring of a beeper will obviously be desirable since it may be useful, even critical, to monitor the beeper to determine that it is actually located in a place not open to visual surveillance").

Karo controls. When tracking a cell phone through cell-site data, the Government will have no way of knowing in advance whether only public information will be revealed or whether private information will be discovered as well. While some monitoring will occur while the target is in a location visible from a public place, much of it will occur while the target is in a private home given a cell phone's small size and portability. Because monitoring of a "beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment," id. at 714, the Government must obtain a search warrant before

using cell-site data to track a target. Id. at 715-17; see Texas Op. 16 ("As 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.").

2. Cell-Site Information Is Not Analogous to Information Revealed by a Traditional Pen/Trap Device.

Despite the clear holding of Karo, the Government insists that "there is no [] reasonable expectation of privacy in the case of cell-site information under the rule articulated in Smith v. Maryland, 442 U.S. 735 (1979)." Gov. Br. 11. Smith held that no Fourth Amendment interests were implicated by the police's placement of a traditional pen register device on Smith's phone, which revealed only the telephone numbers dialed by Smith from his phone.

Smith explained that the defendant had no expectation of privacy in the numbers he voluntarily dialed because "all telephone users realize that they must convey phone numbers to the telephone company." 442 U.S. at 742. A telephone user "voluntarily convey[s] numerical information to the telephone company" when he uses his phone to make a call, and thus "assume[s] the risk that the company would reveal to the police the numbers he dialed." Id. at 744.

There is a world of difference, however, between the use of a simple pen register in Smith and the use of cell-site data emanating from a cell phone -- even when not in active use -- to track a target's movements. First and foremost, "[u]nlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company." Texas Op. 15. As noted, cell-site data can be obtained regardless of whether the user is making a call or receiving a call. E.g., Note, supra, at 316 ("[S]ervice carriers can determine [cell-site location] information with surprising ease whenever cell phones are turned on . . . ."). The information desired by the Government, unlike that at issue in Smith, is in no way "voluntarily conveyed" by the user to the cell provider. Indeed, the Sixth Circuit rejected the Government's attempt to analogize cell-site data with the simple pen register

data discussed in Smith on this very ground. Forest, 355 F.3d at 951 ("Unlike the defendant in Smith, Garner points out that 'he did not voluntarily convey his cell site data to anyone.'"); see also Note, supra, at 315 ("The decision [by cell phone users] not to make or answer phone calls [] supports an argument . . . that [they] should have constitutional protection because they sought to preserve their cell phone information as private . . . .").

Moreover, the Government makes no effort to show that all or even most cell phone users realize that they are conveying their location and movements to their cell phone company simply by leaving their phones on. Indeed, an informal survey conducted in this Office confirms that most cell users are quite surprised to learn that the phone company can "creat[e] a virtual map of [his or her] movements" so long as the user does not turn off his or her phone, regardless of whether he or she initiates or receives an actual call. Note, supra, at 309. "While society may be willing to accept the idea of collecting information associated with the origination and termination of calls," in sum, "people are likely to reject the prospect of turning every cell phone into a tracking device." Id. at 316.

Karo, not Smith, controls. The Government must therefore obtain a search warrant before it can obtain cell-site data for the target phone.

Respectfully submitted

YUANCHUNG LEE
Assistant Federal Defender
Tel.: (212) 417-8742

cc: Thomas G.A. Brown, Esq.
Assistant United States Attorney
United States Attorney's Office
Southern District of New York
One St. Andrew's Plaza
New York, NY 10007
(BY HAND)

cc: Honorable Gabriel W. Gorenstein
United States Magistrate Judge
Southern District of New York
500 Pearl Street
New York, NY 10007
(BY HAND)