U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

COPY

October 5, 2005

By Hand

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

Re: Application for Pen Register and Trap and Trace Device With Cell-site Location Authority

Dear Magistrate Judge Peck:

The Government respectfully submits this letter in response to Your Honor's request for briefing before deciding whether to approve further Government applications for orders to disclose cell-site information. For the reasons set forth below, the Court should grant such applications pursuant to the combined authority of Title 18, United States Code, Sections 3121, et seq. (the pen register and trap and trace statute, or "Pen/Trap Statute"), and Title 18, United States Code, Sections 2701, et seq. (the Stored Communications Act, or "SCA").

BACKGROUND

A. Cellular Telephone Networks

Cellular telephone networks function 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. As the cell phone and its user move from place to place, the cell phone automatically switches to the cell tower that provides the best reception. For this process to function correctly, the cell phone must transmit a signal to a nearby cell tower to register its presence within the cell network. Cellular telephone companies typically keep track of this information, which can include the identity of the cell tower currently serving the cell phone and the portion of the tower facing it, in order to provide service to the cell

phone. Cellular telephone companies also have the technical means to collect and store this information.

B. Orders to Compel Disclosure of Cell-site Data

The United States Attorney's Office for the Southern District of New York - like other U.S. Attorney's offices around the country - has routinely applied for and obtained court orders for pen registers and trap and trace devices with cell-site disclosure authority ("cell-site orders"). These orders compel cellular telephone companies to report dialed and received numbers, as well as cell-site data, for a particular cell phone on a prospective basis. The cell-site information is used by government agents to, among other things, help locate kidnaping victims and fugitives or other targets of criminal investigations.

In its applications, the U.S. Attorney's Office for the Southern District of New York relies on a combination of two statutes to authorize the disclosure of cell-site information: Title 18, United States Code, Sections 3121, et seq., (the Pen/Trap Statute) and Title 18, United States Code, Sections 2701, et seq., (the SCA), in particular Section 2703(d).[1] As discussed more fully below, a pen register/trap and trace device may be issued upon a Government attorney's affirmation "that the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122. Cell-site disclosure requires a further demonstration by the Government attorney 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 or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). It is this Office's practice to comply with these requirements when submitting an application for cell-site orders.

[1] It is this Office's understanding that the U.S. Attorney's Office for the Eastern District of New York likewise relied on the same combination of statutes in its application for a cell-site order which was rejected by Magistrate Judge Orenstein, as discussed below.

C. The Government's Recent Applications for Cell-site Orders

On September 21, 2005, the Government submitted two sealed applications for cell-site orders. (A copy of a similar model application is attached hereto as Exhibit A.) On September 22, 2005, Your Honor's chambers informed the Government that Your Honor had declined to grant the Government's applications without further briefing from the Government concerning the propriety of issuing these orders. In doing so, Your Honor's chambers cited a recent opinion by Magistrate Judge Orenstein in the Eastern District of New York, In re Authorizing the Use of a Pen Register, 2005 WL 2043543 (E.D.N.Y. Aug. 25, 2005).

D. Magistrate Judge Orenstein's Opinion

In his decision, Magistrate Judge Orenstein rejected a Government application for a cell-site order, finding that neither Section 2703(d) nor the Pen/Trap Statute standing alone provided sufficient authority for the disclosure of cell-site data, and that a search warrant issued on a showing of probable cause would be required for this information. Notably, Judge Orenstein did not consider whether the statutes together provided the necessary authority.

Referring to the language in Section 2703(d), Judge Orenstein stated that "the only one" of Section 2703's provisions that "appears arguably to permit the disclosure of cell-site location information is the language permitting the disclosure of 'the contents of a wire or electronic communication.'" In re Pen Register, 2005 WL 2043543 at *1-2 (emphasis added". Judge Orenstein concluded that this language was insufficient, however, finding that cell-site information constitutes a "communication from a tracking device," as defined in 18 U.S.C. § 3117, which is specifically exempted from the class of "electronic communications" discoverable under Section 2703. Id. (citing 18 U.S.C. §§ 2510(12)(C)). The Court ended its analysis by contending that use of a tracking device normally requires a showing of probable cause.

Turning to the Pen/Trap Statute, Judge Orenstein recognized that pen registers and trap and trace devices provide cell-site information as a matter of course. Id. at *2. The Court found, however, that the Pen/Trap Statute was limited by Section 103(a)(2) of the Communications Assistance for Law Enforcement Act ("CALEA"), P.L. 103-313, 108 Sta. 4279 (1994), codified at 47

U.S.C. § 1002(a)(2)(B), which provides that "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber." 47 U.S.C. § 1002(a)(2)(B) (emphasis added). On this basis, Judge Orenstein determined that the Pen/Trap Statute did not provide authority for the disclosure of cell-site information, which would disclose the physical location of a cell phone user, and again suggested that probable cause is required to obtain this information.

The United States Attorney's Office for the Eastern District of New York has moved Magistrate Judge Orenstein to reconsider his opinion, and the matter is presently sub judice.

DISCUSSION

This Court should decline to follow Judge Orenstein's reasoning because it is based upon a flawed understanding of the relevant statutes. As a threshold matter, cell-site information is properly classified as "information pertaining to a subscriber" pursuant to Section 2703(c), not the "contents of an electronic communication" under 18 U.S.C. §§ 2703(a) or (b), as Judge Orenstein has concluded.[2] Further, cell-site information is not the product of a "tracking device" or communications from it. Instead, as discussed below, Section 2703(d) by itself, upon a showing of specific and articulable facts demonstrating reasonable grounds to believe the information sought is relevant and material to an ongoing investigation, authorizes the disclosure of existing cell-site records. Moreover, Section 2703(d), together with the Pen/Trap Statute and upon a showing of the necessary specific and articulable facts, authorizes the disclosure of prospective cell-site information, as the Government has sought in its recent applications to this Court.

[2] On September 19, 2005, Judge Orenstein issued an order allowing additional briefing, in which he admitted that his conclusion that cell-site data constitutes the "contents of a communication" is "clearly erroneous." A discussion of the reasons why his conclusion is error is included in this letter brief for Your Honor's reference.

A. Cell-Site Data Are "Records or Other Information" Disclosable Pursuant to 18 U.S.C. § 2703

In rejecting Section 2703(d) as a basis for disclosing cell-site information, Judge Orenstein first posited that only the portion of that statute relating to the "contents of a wire or electronic communication" could arguably provide that authority. This assumption, upon which the rest of Judge Orenstein's conclusion is based, is error. As explained below, it both misconstrues the nature of cell-site data and ignores 18 U.S.C. 2703(c)(1)(B), a statute which, in conjunction with Section 2703(d), authorizes the disclosure of cell-site records.

As an initial matter, cell-site information is not "the contents of a communication" within the meaning of 18 U.S.C. §§ 2703(a) and (b). In general, such "contents" include only the "substance, purport or meaning of a communication." 18 U.S.C. § 2510(8), incorporated by reference in the SCA at 18 U.S.C. § 2711(1). Cell-site information, by contrast, conveys data concerning the particular location a cell phone and its user are in, rather than the contents of any conversations the user has over the cell phone. Thus, cell-site information constitutes "information pertaining to a subscriber," rather than the "contents of a communication." Accordingly, it is governed by Section 2703(c) of the SCA.

The structure of SCA, as it was first enacted and as it was later amended by CALEA, demonstrates that Congress intended to authorize courts to order the disclosure of a broad array of non-content information, such as cell-site information, pursuant to Section 2703(c). When the SCA was enacted in 1986, it permitted the disclosure pursuant to court order or subpoena of a catch-all category of "record[s] or other information pertaining to a subscriber or customer of such service (not including the contents of communications)." See P.L. 99-508, 100 Stat. 1848, 1862 (1986), now codified at 18 U.S.C. § 2703(c)(1). The accompanying 1986 Senate report emphasized the breadth of the "record or other information" language: "[t]he information involved is information about the customer's use of the service not the content of the customers communications." S. Rep. No. 541, 99th Cong., 2d Sess. at 38 (1986).

When Congress enacted CALEA in 1994, it amended the SCA to increase privacy protections with respect to detailed, non-content telephone transactional records. At the same time, however, Congress preserved the Government's right to access such

data. In particular, CALEA created a distinction between basic subscriber records (e.g., a subscriber's name and address and duration of calls) and more detailed transactional logs. Basic subscriber information could be obtained by subpoena. See 18 U.S.C. § 2703(c)(2). Disclosure of "record[s] or other transactional information pertaining to a subscriber to or customer of such service (not including the contents of communications)" other than basic subscriber information, however, required an order pursuant to Section 2703(d). See 18 U.S.C. § 2703(c)(1)(B). To obtain a Section 2703(d) order, the government must offer "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The legislative record reveals that Congress intended this new "intermediate standard," which is midway between the standards required for the issuance of a subpoena and the issuance of a search warrant, see H.R. Rep. No. 827(I), 103rd Cong., 2d Sess., at 31 (1994) (the "House CALEA Report"), to apply to detailed transactional data, such as cell-site information. In discussing the changes to Section 2703(c), the House CALEA Report addressed, in particular, "transactional records from on-line communication services" and acknowledged that they would "reveal more than telephone records or mail records." House CALEA Report at 31. Accordingly, under the revised 2703(c), the Government would now be permitted to obtain the addresses used in e-mail messages, as long as it satisfied the "reasonable grounds" requirement of Section 2703(d). House CALEA Report at 31.

If anything, an individual's privacy interest in the addresses of her e-mail correspondents exceeds her privacy interest in the neighborhood in which she uses a cell phone. Given that Congress explicitly stated that the SCA, as amended by CALEA, was intended to authorize the disclosure of e-mail addresses pursuant to Section 2703(d), it likewise intended that statute to govern less intrusive categories of detailed, non-content telephone transactional records, such as cell-site information.

B. Prospective Disclosure of Cell-Site Data Is Authorized Pursuant to the Pen/Trap Statute and Section 2703(d)

Judge Orenstein also denied the Government's application for a cell-site orders on the theory that CALEA prohibits use of the Pen/Trap Statute to acquire prospective cell-site information. In re Pen Application at *3-4. This, too, is error because it fails to consider the Pen/Trap Statute together with Section 2703(d), a combination which provides authority for the prospective disclosure of cell-site data.

When the Pen/Trap Statute was first enacted in 1986, pen registers and trap and trace devices were given narrow definitions which were limited to the capture of telephone numbers. For example, "pen register" was defined in part to mean "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 . . . ." Electronic Communications Privacy Act of 1986, § 301, Pub. L. No. 99-508, 100 Stat. 1848 (1986). As communications networks developed, however, federal law enforcement began to use pen/trap orders to collect additional categories of non-content information. For example, a pen/trap order was used on an e-mail account to locate a murder suspect who had evaded capture for three years. See Fighting Cyber Crime: Hearing Before the Subcommittee on Crime of the Committee on the Judiciary, 107th Cong., 1st Sess. 47-48 (2001) (statement of Michael Chertoff, Asst. Atty General, Crim. Div., U.S. Dept. of Justice) (available at judiciary.house.gov/legacy/chertoff_061201.htm).

Any ambiguity over whether pen registers and trap and trace devices were narrowly limited to telephone numbers was eliminated by the USA PATRIOT Act of 2001 § 216, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("Patriot Act"). The Patriot Act amended the definitions of "pen register" and "trap and trace device" to make clear that the Pen/Trap Statute applies to a broad variety of communications technologies and allows the collection of a broad range of non-content information. "Pen register" is now defined to mean

> 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 . . . .

18 U.S.C. 3127(3). Similarly, "trap and trace device" is now defined to mean

> 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, provided, however, that such information shall not include the contents of any communication.

18 U.S.C. § 3127(4).

Prospective cell-site collection falls within the scope of these definitions of "pen register" and "trap and trace device" because cell-site information constitutes "dialing, routing, addressing, and signaling information." In particular, cell-site information is used by cell phone companies to route calls to and from their proper destination. The House Report on the bill that became the Patriot Act emphasized the inclusion of cell-site data within the scope of the Pen/Trap Statute when it noted 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." H.R. Rep. No. 236(I), 107th Cong. 1st Sess. at 53 (2001). The Report further explained the broad scope of information that may be obtained by pen registers/trap and trace devices: "This concept, 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." Id. Accordingly, the Government must seek a pen/trap order to collect cell-site data. See 18 U.S.C. 3121(a) ("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 . . . .")

The Government, however, cannot rely upon the Pen/Trap Statute alone because CALEA restricts the use of pen/trap orders to obtain cell-site information. It is critical to note, however, the mechanism through which Congress accomplished this restriction. Congress did not – as Judge Orenstein presumes – simply forbid the use of pen/trap orders to obtain such information. Instead, it prohibited the disclosure of cell-site information "solely pursuant" to a pen/trap order:

> (a) ... 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 - . . .
>
> > (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, United States Code), 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). . . .

CALEA § 103(a), codified at 47 U.S.C. § 1002.

There is no dispute that "[i]nformation that may disclose the physical location of the subscriber" includes cell-site information of the kind in issue here. Congress' use of the "solely pursuant" language to restrict the use of pen/trap orders to obtain cell-site information, however, demonstrates that the Pen/Trap Statute applies to the collection of cell-site information, as discussed above, but that additional authority beyond the Pen/Trap Statute should be sought for such collection. In fact, as discussed at pages 5-6 above, CALEA created just such authority when it amended the SCA to authorize the disclosure of cell-site information pursuant to 18 U.S.C. §§ 2703(c)(1)(B) and 2703(d), provided the Government articulates facts demonstrating "reasonable grounds to believe" that the information sought is "relevant and material" to a criminal investigation. 18 U.S.C. § 2703(d). Thus, by amending the SCA, CALEA created authority distinct from the Pen/Trap Statute - i.e., not "solely pursuant" to that statute - that authorizes the release to the Government of "information that may disclose the physical location of" a cell phone subscriber.

Indeed, the only conceivable purpose for the "solely pursuant" language is to make clear that cell phone service

providers must disclose cell-site data when authority in addition to the Pen/Trap Statute is relied upon by the Government. Section 2703(d) provides that authority, as is clear from the nature of cell-site information, the structure and legislative history of the SCA, and by the timing of Section 2703(d)'s introduction at the same time CALEA's restrictive language was enacted. Any argument that the Pen/Trap Statute and Section 2703(d) cannot be combined would render the "solely pursuant" language surplusage, a result which Congress could not have intended. It also suggests the absurd result that the Government, once it had obtained a pen/trap order, would be barred from obtaining cell-site data, no matter what additional authority it cited, including a search warrant.

Here, the U.S. Attorney's Office for the Southern District of New York has not sought to acquire cell-site information "solely pursuant" to the Pen/Trap Statue, but under the more demanding requirements of Section 2703(d) as well, consistent with CALEA. (See Exhibit A at 2-3). Under the Pen/Trap Statute, a court is empowered to authorize the installation of a pen register or trap and trace device upon the finding that a law enforcement officer "has certified . . . that the information sought is likely to be obtained . . . is relevant to an ongoing investigation." 18 U.S.C. § 3123(b). Recognizing the complementary role played by the SCA, and to comply with CALEA, 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" that 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.

C. Disclosure of Cell-Site Information Does Not Convert a Cell Phone Into a "Tracking Device" Requiring a Warrant

Judge Orenstein also concluded, in the course of rejecting the Government's application for a cell-site order, that disclosure of cell-site information pursuant to Section 2703(d) "would effectively allow the installation of a tracking device without the showing of probable cause normally required for a warrant." In re Pen Application at *2. Judge Orenstein amplified his point by asserting that cell-site information is the equivalent of "physical surveillance of the telephone user" because "it reveals [the user's] location at a given time." Id. This reasoning is incorrect.

First, a warrant is generally not required for the installation of a tracking device. See United States v. Knotts, 460 U.S. 276 (1983) (holding that law enforcement need not obtain a warrant to install a proximity beeper that discloses the location of a car traveling on public roads). In fact, there is no warrant requirement under the tracking device statute, 18 U.S.C. § 3117. See United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000) ("But by contrast to statutes governing other kinds of electronic surveillance devices, section 3117 does not prohibit the use of a tracking device in the absence of conformity with the section.") (emphasis in original).

Second, a warrant is required for a mobile tracking device only when the Government invades a reasonable expectation of privacy. Compare United States v. Knotts, 460 U.S. at 285 with United States v. Karo, 468 U.S. 705, 713-18 (1984) (holding that warrantless use of a beeper inside a house violated Fourth Amendment). However, there is no such reasonable expectation of privacy in the case of cell-site information under the rule articulated in Smith v. Maryland, 442 U.S. 735 (1979). In Smith, the Supreme Court applied a two-prong test to determine whether a defendant had a reasonable expectation of privacy in dialed telephone numbers. Under the first prong, the Court determines whether a defendant exhibits an actual (subjective) expectation of privacy. Under the second prong, the Court then determines whether such a subjective expectation of privacy is one that society is prepared to recognize as reasonable. See Smith, 442 U.S. at 742-44. A reasonable expectation of privacy exists only if both of these criteria are met.

In Smith, the Supreme Court held both that telephone users had no subjective expectations of privacy in dialed telephone numbers and that any such expectation is not one that society was prepared to recognize as reasonable. The Court stated: "First, we doubt that people in general entertain any actual expectation in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Smith, 442 U.S. at 742. Notably, the Supreme Court based this statement about subjective expectations of privacy not on any public survey or polling data, but from the way telephones function. The Court went on to state that "even if [a defendant] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable."

Smith, 442 U.S. at 743 (internal quotes omitted). It noted that "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith 442 U.S. at 743-44. In Smith, the user "voluntarily conveyed numerical information to the telephone company" and thereby "assumed the risk that the company would reveal to the police the numbers he dialed." Smith 442 U.S. at 744.

This reasoning is equally applicable to cell phone usage. Cell phone users understand that they are broadcasting a signal to the cell phone company so that the cell phone company can locate them to complete their calls. Users cannot have a subjective expectation that the location of the cell tower through which the signal is passed will be secret from the cell phone company. Moreover, even if users did have such an expectation, it would make no difference under the second prong of Smith's analysis. A cell phone user voluntarily transmits a signal to the cell phone company, and thereby "assumes the risk" that the cell phone provider will reveal to law enforcement the cell-site information. This is not a privacy expectation that society is prepared to view as reasonable. Indeed, the cell-site information here is even less worthy of protection than the dialed telephone numbers in Smith. There, the defendant was claiming a privacy interest in numbers he personally had dialed. In cell-site cases, a defendant must attempt to claim a privacy interest in information generated by the cell phone provider and which he never possessed - the location of the cell towers that received a signal the user voluntarily broadcast.

Third, a cell phone disclosing cell-site data does not fit the definition of a "tracking device." A tracking device is "an electronic or mechanical device which permits the tracking of movement of a person or object." 18 U.S.C. § 3117(b). In other words, it is a homing device which allows law enforcement to closely monitor its physical location and the location of the person or thing to which it is attached. Cell-site data, while it provides information about the location of the cell phone and its user, does not permit detailed, continuous tracking of the cell phone user's movement. At best, it can provide a cell phone and it's user's general location within a broad area surrounding a particular cell-site tower, or show when a cell phone moves to an adjoining cell. Indeed, as long as the cell phone user stays within reception of a particular cell tower, it is impossible to determine the user's precise location, or even whether the user is stationary or moving. Thus, cell-site data does not actually

"permit the tracking of the movement of a person or object," and certainly does not replace "physical surveillance" which would disclose a person's location at a particular moment, as Judge Orenstein presumes it would. In re Pen Application at *2.

Moreover, the legislative history of the Electronic Communications Privacy Act ("ECPA"), see § 108, Pub. L. No. 99-508, 100 Stat. 1848 (1986), which enacted the tracking device statute codified at 18 U.S.C. § 3117, demonstrates that Congress understood "tracking devices" to be homing devices which are separate and apart from cell phones. For example, the Senate Report on ECPA includes a glossary of technological terms. The glossary - which defines "electronic tracking devices" separately from cell phones and pagers - defines electronic tracking devices as

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

S. Rep. No. 541, 99th Cong., 2d Sess., at 10 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564 (1986).

There is no reason to supply a broader definition of "tracking device" than Congress intended. If "tracking device" were given the broad interpretation suggested by Judge Orenstein, nearly all communications devices would be tracking devices. Certainly any device relying on a cellular communication system, including many pagers, text messaging devices such as Blackberries, and cellular Internet systems would, like cell phones, be a tracking device. Moreover, it is generally possible to determine the physical location of users connected to the Internet, making all computers which communicate over the Internet tracking devices, according to Judge Orenstein's definition. Similarly, land-line telephones would also constitute tracking devices, because it is possible to determine an individual's location from his use of a land-line telephone.

CONCLUSION

For the foregoing reasons, the Court has authority to authorize the disclosure of cell-site information upon the showings required by the Pen/Trap Statute and Section 2703(d) of the SCA. Accordingly, the Government respectfully requests that the Court grant is applications for cell-site orders.

Respectfully submitted,

MICHAEL J. GARCIA
United States Attorney

By: Thomas G. A. Brown
Thomas G. A. Brown
Assistant United States Attorney
(212) 637-2194