U.S. Department of Justice

Executive Office for United States Attorneys
Freedom of Information/Privacy Act Staff
600 E Street, N.W., Room 7300
Washington, D.C. 20530
202-616-6757 Fax 202-616-6478

Requester: Marcia Hofmann

Request Number: 08-4268-R

Government Component that referred material: U.. S. Department of Justice, Criminal Division

Dear Requester:

This is in reply to your Freedom of Information Act/Privacy Act request of September 22, 2006. Records were referred to us by the government component above for direct response to you.

The referred material has been considered under both the FOIA and the Privacy Act to provide you the greatest degree of access. Exemptions have been applied when deemed appropriate either for withholding records in full or for excising certain information. The exemptions cited are marked below. An enclosure to this letter explains the exemptions in more detail.

Section 552			Section 552a
[ ] (b)(1)	[ ] (b)(4)	[ ] (b)(7)(B)	[**X**] (j)(2)
[ ] (b)(2)	[ ] (b)(5)	[**X**] (b)(7)(C)	[ ] (k)(2)
[ ] (b)(3)	[ ] (b)(6)	[ ] (b)(7)(D)	[ ] (k)(5)
_____	[ ] (b)(7)(A)	[ ] (b)(7)(E)	[ ] _____
_____		[ ] (b)(7)(F)	

We have reviewed approximately 78 page(s) of material:

3 page(s) are being released in full (RIF);
44 page(s) are being released in part (RIP);
_____ page(s) are withheld in full (WIF) and
31 pages were not originated within our agency and are being returned to Department of Justice, Criminal Division. The document should be referred to OIP.

This is the final action on this above-numbered request. You may appeal this decision on this request by writing within 60 days from the date of this letter to the **Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001**. Both the letter and envelope should be marked "FOIA Appeal." If you are dissatisfied with the results of any such administrative appeal, judicial review may thereafter be available in U.S. District Court, 28 C.F.R. §16.9.

Sincerely,

William G. Stewart II
Assistant Director

Enclosure(s)

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

(b) (1) (A) specifically authorized under criteria established by and Executive order to be kept secret in the in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

PRIVACY ACT: TITLE 5, UNITED STATES CODE, SECTION 552a

(d)(5) information complied in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to Executive Order 12356 in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material complied for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability eligibility, or qualification for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his identity would be held in confidence.

REQUESTER: Marcia Hofmann

FOIA FILE#: 08-4268-R

DOCUMENTS Released in Full "RIF"

1 pages

U.S. Department of Justice

Executive Office for United States Attorneys

Office of the Director

Room 2244A, Main Justice Building
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530

(202) 514-2121

MEMORANDUM - Sent via Electronic Mail

DATE: JUN 3 2002

TO: All United States Attorneys
All First Assistant United States Attorneys
All Criminal Chiefs

FROM: Lynne M. Halbrooks
Kenneth L. Wainstein
Director

SUBJECT: Policy Concerning Operation of Pen Registers and Trap and Trace Devices

ACTION REQUIRED: None. Information only.

CONTACT PERSON: Chris Chaney
Counsel to the Director Staff
(202) 514-1023
E-mail: chaney, chris

The attached memorandum from Deputy Attorney General Larry D. Thompson sets forth the Department's policy concerning the avoidance of "overcollection" in the use of pen registers and trap and trace devices. Please distribute this memorandum to all criminal Assistant United States Attorneys and other appropriate personnel. If you have questions or comments, please contact Chris Chaney. Thank you.

Attachment

cc: United States Attorneys' Secretaries

RIF

REQUESTER: Marcia Hofmann

FOIA FILE#: 08-4268-R

MIXED DOCUMENTS

Pages RIF 2

Pages RIP 44

Pages WIF _____

DUP Pages _____

U.S. Department of Justice

Michael J. Sullivan
United States Attorney
District of Massachusetts

Main Reception: (617) 748-3100

John Joseph Moakley United States Courthouse
1 Courthouse Way
Suite 9200
Boston, Massachusetts 02210

November 15, 2005

Charles B. Swartwood, III
Chief, United States Magistrate Judge
United States District Court
District of Massachusetts
1 Courthouse Way
Boston, MA 02210

Re: Pen Register/Trap & Trace Orders

Dear Judge Swartwood:

Thank you for the opportunity to address the issues raised by the Memorandum and Order entered by United States Magistrate (7C)

(7C) We very much share (7C) concern to minimize the interception of content during the execution of pen register and/or trap & trace orders. However, for the reasons articulated below, we believe that (7C) supplemental language is contrary to the statutory balance determined by Congress as set forth in 18 U.S.C. §3121(c). In addition, the definition of "contents" proposed by (7C) will be overly broad when it is applied in certain network contexts. Accordingly, we believe the Court should not adopt this supplemental language as a model.

(7C) added the following supplemental language to the trap and trace orders presented to him in Docket No. (7C)

> It is ORDERED that the pen register and trap and trace device installed in accordance with the within Order be configured to <u>exclude all information constituting or disclosing the "contents"</u> of any communications or accompanying electronic files.

RIP
7C

> "Contents" is defined by statute as any "...information concerning the substance, purport or meaning of that communication."
>
> The disclosure of the "contents" of communications is prohibited pursuant to this Order even if what is disclosed is also "dialing, routing, addressing and signaling information."
>
> Therefore, the term "contents" of communications includes subject lines, application commands, search queries, requested file names, and file paths. Disclosure of such information is prohibited by the within Order.
>
> Violation of the within Order may subject an internet service provider to contempt of court sanctions.
>
> In implementing the within Order, should any questions arise as to whether the pen register and/or trap and trace device should be configured to provide or not to provide any particular category of information over and above those stated, the Trial Attorney and/or the internet service provider are invited to apply to this court for clarification and/or guidance. [emphasis added]

Three aspects of this supplemental language are of concern: (1) it imposes an absolute bar on even incidental acquisition of content, overriding Congress' explicit acknowledgment that technical complications may make such incidental collection unavoidable; (2) it shifts the statutory burden of minimizing the interception of the contents of communications from the applicant government agency to the internet service provider ("ISP"); and (3) it establishes an overly broad itemization of "contents" which includes non-content material. These aspects are addressed below after a description of the central statutory provision, 18 U.S.C. §3121(c).

RIF

As (7C) identified, the nettlesome line between content and non-content surfaced first in the area of telecommunications the better part of a decade ago. At that time, individuals had begun with increasing frequency to use their telephones to access banking and credit card information, keying in their account numbers for this purpose. In its second session, the 103th Congress amended the pen register statute in 1994 to limit, but not prohibit, the interception of content during the execution of a pen register. The limitation established by Congress, and the burden of compliance with that limitation, was codified in §3121(c) as follows:

> (c) **Limitation** - A Government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

After seven years' experience with this formulation, Congress amended the statute again in 2001 in the Patriot Act, keeping the same core approach, but expanding §3121(c) to explicitly include trap and trace devices, and the placement of both pen registers and trap and trace devices on electronic networks:

> (c) **Limitation** - A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications. [emphasis added]

This is the specific statutory provision which the Court is seeking to implement.

RIP
7C

supplemental language directly conflicts with 18 U.S.C. 3121(c) in two respects. First, Order converts the statutory requirement to use "technology reasonably available" to avoid content into an absolute ban on the interception of content. Congress recognized - in its revisions to the pen register statue in both 1994 and 2001 - that the complexity of telecommunications and network communications presently create impossible challenges to separating all content from non-content dialing, routing, addressing and signaling information in real time. Accordingly, rather than subjecting government agencies (or, in the case order, internet service providers) to the risk of contempt of court when content was inevitably intercepted as part of the execution of a pen register or trap and trace order, Congress established the more elastic requirement in §3121(c) that the government use "technology reasonably available to it" to accomplish this end. Thus, we believe, the language in Order exceeds the authority conferred by the statute.

As we indicated in the beginning of this letter, the Department of Justice shares the Court's deep concern that the collection of content in the operation of pen registers and trap and trace devices be avoided and minimized to the extent technologically possible. Accordingly, in May, 2002, then Deputy Attorney General Larry D. Thompson issued a memorandum setting forth the Department's policy regarding the avoidance of "over-collection" in the use of pen registers and trap and trace devices that are deployed under the authority of 18 U.S.C. §3121 et seq. In sum, the memorandum establishes the following basic principles: that reasonably available technology shall be used to avoid over-collection; and, when over-collection does occur despite use of reasonably available technology, no affirmative investigative use shall be made of that information except to prevent immediate danger of death, serious physical injury, or harm to the national security. I have attached to this letter a copy of the 2002 policy memorandum for the Court's consideration.

Our second concern is that by its express terms, §3121(c) places the burden on the government agency to ensure that the amount of content inadvertently intercepted pursuant to a pen register or trap and trace order is minimized. By contrast,

RIP

(7C) Order puts the ISP at risk of contempt of court sanctions if the pen register and trap and trace device is not configured to exclude absolutely all contents including, but importantly not limited to, things listed in the Order. We believe this burden on the ISP is beyond the authority conferred by the statute. Further, internet service providers vary in their technical capacity to install network pen register and trap and trace devices. ISPs receiving Orders with this supplemental language will be unable to guarantee compliance - - particularly, given the vagaries (discussed below) of what is content - - and will therefore be unwilling to install pen registers or trap and trace devices as a matter of prudence.

Our third concern is the Order's overbroad definition of content, which will prevent the collection of needed non-content material in a number of contexts. The term "contents" is defined in the Order as including "subject lines, application commands, search queries, requested file names, and file paths." Disclosure of such information is prohibited by the Order.

Context is critical to determining whether information being transmitted over the internet is content or non-content. Had (7C) definition of "content" only dealt with e-mail traffic, portions of the definition would have been technically accurate, while others would have been superfluous to the applications before him. Without question, the subject line of an email is "content," as is the body of the text, while the addressee's identification and the sender's identification are not. Search queries, requested file names and file paths are not found in typical e-mail traffic other than in the body of the text.

Depending on context, "requested file names" may or may not be content. The name of a file mentioned in the body of an email, for instance, would be content. By contrast, log files on a web server - listing the date, time, filename, and remote network address for each file request received by the server - are non-content transactional records. The same is true for "file paths."

The application of the term "search queries" is similarly ambiguous. In the web search context, some queries - notably of

RIP
7C

Google - result in URLs such as http://www.google.com/search?q=red+sox. Here, the parameters included in the URL after the question mark ("q=red+sox") are certainly content. However, what is left of the question mark, "http://www.google.com/search," is nothing more than an identifier of the location of a network resource - that is, a non-content address.

We submit that 726 Order fails to recognize these important context dependent distinctions, and that district-wide adoption of his addendum would be both imprudent and inconsistent with the pen/trap statute. To the extent that there are difficult issues to resolve concerning the definition of "content," we believe those issues should be decided acquisition by acquisition in specific factual and technological contexts, rather than pre-formulated in necessarily imprecise and unclear, blanket prohibitions appended to every order.

The government does not seek, through pen register or trap and trace orders, to obtain the right to collect content. The wiretap statute and other vehicles are appropriate for this. Rather, in enacting the pen register statute, Congress has established a means for the Government to collect non-content information. At the same time, Congress has recognized that certain content may necessarily be incidentally collected because of the limitations of presently available technology, and has approved such incidental collection to the extent necessary to using pen register and trap and trace devices effectively.

Once again, thank you for the opportunity to address the Court on this important matter. Should it be of use to the Court, please let me know if you or any of the other Magistrate Judges would like to discuss this matter further with this office

RIP
7c

or receive a briefing on any of the technology at issue.

Very truly yours,

MICHAEL J. SULLIVAN
United States Attorney

By: _____
MICHAEL K. LOUCKS
First Assistant U.S. Attorney

RIF

U.S. Departm. . 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

October 5, 2005

By Hand

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

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 ( ) as discussed below.

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

On (7C), the Government submitted two sealed applications for cell-site orders. (A copy of a similar model application is attached hereto as Exhibit A.) On 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 (7C) in the Eastern District of New York, (7C)

D. Magistrate Judge Orenstein's Opinion

In his decision, (7C) 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, (7C) (7C) did not consider whether the statutes together provided the necessary authority.

Referring to the language in Section 2703(d) (7C) (7C) 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.'" (7C) at *1-2 (emphasis added". (7C) 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, (7C) 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

RIP
7C

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 (7C) to reconsider his opinion, and the matter is presently sub judice.

DISCUSSION

This Court should decline to follow (7C) 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 (7C) 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 (7C) 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.

RTP

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, (7C) 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 (7C) 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

RIP 7C

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.

RIP

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

(7C) 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. (7C) 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 . . . .

RFP 7C

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 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

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." 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

RIP

"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 presumes it would.

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.

RIP

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: _____
Assistant United States Attorney

RIP

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

November 22, 2005

By Hand

Chief United States Magistrate Judge
Southern District of New York
United States Courthouse
500 Pearl Street, Rm. 750
New York, New York 10007

Re: Applications for Pen Registers and Trap and Trace Devices With Cell-site Location Authority

Dear Chief Magistrate Judge Peck:

The Government respectfully submits this letter in response to the request of [redacted] on behalf of Your Honor, for further briefing concerning the Court's authority to order the prospective disclosure of cell-site information. Specifically, this letter addresses two opinions recently issued by [redacted] in the Southern District of Texas and [redacted] in the Eastern District of New York, which called into question the Government's position concerning this authority.

[redacted] ("New York Op."). This letter also responds to an October 27, 2005 amicus curiae submission from the Federal Defenders of New York, Inc. (the "Federal Defenders"), which largely repeats the reasoning of these opinions and adopts their conclusions (the "Fed. Def. Br.").

In an October 5, 2005 letter to the Court (the "October 5 Letter"), the Government set forth in detail the reasons why the prospective disclosure of cell-site information may be obtained pursuant to the combined authority of Title 18, United States Code, Sections 3121, et seq. (the "Pen/Trap Statute"), and

RIP

Section 2703 of the Stored Communications Act ("SCA"), Title 18, United States Code, Sections 2701, et seq.

The Government's position may be summarized as follows: The prospective disclosure of cell-site information falls squarely within the Pen/Trap Statute because cell-site information is "dialing, routing, addressing, or signaling information," and the provisions of that statute mandate a pen/trap order for such disclosure. See 18 U.S.C. §§ 3121(a), 3127(3), and 3127(4). The Pen/Trap Statute by itself, however, is insufficient authority for such disclosure, because Congress has forbidden a cellphone company from disclosing cell-site information "solely pursuant" to a pen/trap order. See 47 U.S.C. § 1002(a)(2)(B). The necessary authority for the disclosure of cell-site information called for by the Pen/Trap Statute is provided by Section 2703 of the SCA. In particular, cell-site information falls within the scope of the SCA because it constitutes "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication] service (not including the contents of communications)." See 18 U.S.C. § 2703(c)(1). As a result, its disclosure may be obtained pursuant to an "articulable facts" order issued under 18 U.S.C. § 2703(d). Accordingly, the Pen/Trap Statute, together with the SCA, provide authority for the disclosure, on a prospective basis, of cell-site information.

DISCUSSION

The two Magistrate Judges' opinions, as well as the Federal Defenders' brief, challenge the Government's position in three principal ways. First, they dispute the Government's interpretation of the Pen/Trap Statute and the SCA. Their alternative reading, however, is grounded in a misunderstanding of the relevant statutes and legislative history. Second, they reason that cellphones are "tracking devices" and that the tracking device statute, 18 U.S.C. § 3117, requires the Government to seek a warrant based on probable cause for the disclosure of prospective cell-site information. This argument is incorrect for at least two reasons: cellphones do not fall within the purview of the tracking device statute, but even if they did, there is no statutory requirement that the Government seek a warrant. Third, they assert that there is a reasonable expectation of privacy in cell-site information under the Fourth Amendment, which also triggers the need for a warrant issued upon a showing of probable cause. This argument fails because there is no reasonable expectation of privacy in information conveyed to third parties, and cell-site information is plainly data

RIP

conveyed to third-party cellphone companies. Accordingly, this Court should decline to follow the objections to the Government's position that prospective cell-site disclosure is authorized pursuant to the Pen/Trap Statute together with the SCA.

A. Legislative History Supports the Disclosure of Cell-Site Data Pursuant to the Combined Authority of the Pen/Trap Statute and the SCA

It is important to address at the outset what the Magistrate Judges' opinions and the Federal Defenders' brief view to be a critical weakness in the Government's position: that there is a lack of legislative history supporting the Government's argument that prospective cell-site information may be gathered pursuant to Section 2703 of the SCA and the Pen/Trap Statute. See Texas Op. at *15-16; New York Op. at *25; Fed. Def. Br. at 18-19. (7C) quotes extensively from congressional testimony by then-Federal Bureau of Investigation Director Louis Freeh in connection with proposed legislation that became the Communications Assistance for Law Enforcement Act ("CALEA"), P.L. 103-313, 108 Stat. 4279 (1994). (7C) refers in particular to Director Freeh's proposal to Congress of the restriction - later embodied in the "solely pursuant" language of 47 U.S.C. § 1002(a)(2)(B) - on the disclosure of cell-site information pursuant to a pen/trap order. See Texas Op. at *14. Based on this testimony, (7C) concludes that "[w]hile the [solely pursuant] disclaimer did not affirmatively specify what legal authority would govern access to prospective cell site data, Director Freeh's testimony makes clear that an order under SCA § 2703(d) was not a likely suspect." Texas Op. at *15.

(7C) however, fails to take into account all of Director Freeh's testimony on this subject. Significantly, Director Freeh discussed the Government's undisputed ability to obtain "transactional data," such as cell-site information, before proposing the CALEA restriction on which (7C) focuses. Director Freeh's testimony thus makes clear that the SCA provided the necessary authority to secure the disclosure of cell-site data called for by CALEA's limitation. In particular, Director Freeh testified:

> Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this

RIP
7C

> information is not the specific type of information obtained from "true" tracking devices, which can require a warrant or court order when used to track within a private location not open to public view. See United States v. Karo, 469 U.S. 705, 714 (1984). Even when such generalized location information, or any other type of "transactional" information, is obtained from communications service providers, court orders or subpoenas are required and are obtained.

See Police Access to Advanced Communication Systems: Hearings Before the Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary House of Representatives, 103d Cong., 2d Sess. (1994) (statement of Director Freeh), ("Freeh Testimony") available at 1994 WL 223962, at *27-*28. (emphasis added). In the next paragraph of his testimony, Director Freeh proposed the restriction on disclosure of cell-site information which eventually became the "solely pursuant" limitation now codified at 47 U.S.C. § 1002. Id. at *28.

The importance of Director Freeh's testimony cannot be overstated. Director Freeh confirmed the prevailing view of the day, namely, that cell-site information was "transactional information," which could be obtained pursuant to "court orders or subpoenas," not warrants. Indeed, at the time of his testimony, subpoenas could be used to compel disclosure of any non-content records or information under Section 2703(c) of the SCA, although CALEA soon modified this practice. Moreover, "court orders" referred to orders issued pursuant to Section 2703(d), which were used, then as now, to compel disclosure of "a record or other information pertaining to a customer or subscriber." At the time of Director Freeh's testimony, however, such orders were issued upon a showing of relevance to a legitimate law enforcement inquiry, rather than based on the heightened "articulable facts" standard, discussed below. See Electronic Communications Privacy Act of 1986 § 201, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (providing for compelled disclosure of such records when the Government uses a subpoena or "obtains a court order for such disclosure under [18 U.S.C. § 2703(d)]"). See also October 5 Letter at 5. Director Freeh's testimony also made clear that the disclosure of cell-site information did not require a warrant.

RIP
TC

Accordingly, at the moment Director Freeh proposed the limitation on the disclosure of cell-site information pursuant to a pen/trap order, he also made plain to Congress that disclosure of such information was permissible under Section 2703. It is clear from the legislative history, then, that neither Director Freeh nor Congress intended to require warrants for the disclosure of cell-site information. Instead, they intended for the disclosure of such information to be governed by the rules for transactional, non-content information in Section 2703 of the SCA.

It is also important to note, as does, that one of CALEA's goals at the time it was enacted was to preserve the same surveillance capabilities that law enforcement agencies had prior to the advent of cellphones. See Texas Op. at *13-*14. The prospective disclosure of cell-site information under the combined authority of CALEA and the SCA is in keeping with this legislative intent. Under the "old" system of hard-wired telephones, a pen/trap order allowed law enforcement to pinpoint the physical location of a telephone user each time he or she placed a call because landlines, be they payphones or residential telephones, are fixed to a particular address. See United States Telecom Ass'n v. FCC, 227 F.3d 450, 455 (D.C. Cir. 2000). Moreover, law enforcement could obtain this location information on a prospective basis using the information derived pursuant to the Pen/Trap Statute. In contrast, cellphones do not require their users to be in a particular place to send and receive calls. As a result, it is impossible to determine the physical location of a cellphone user without reference to cell-site data.[1] Accordingly, Section 2703(d), together with the Pen/Trap

---

[1] In accordance with CALEA, the telecommunications industry, working with the FBI, adopted a set of technical standards, known as the "J-Standard," to allow law enforcement to maintain the surveillance capability it had before telecommunications technology changed. One of the J-Standard's specifications is that cellphone companies must have the capability to disclose the physical location of the nearest cell-site tower at the beginning and end of each call. See United States Telecom Ass'n v. FCC, 227 F.3d at 455. The J-Standard for cell-site information, at best, discloses the neighborhood a cellphone user is in at the time a call starts and at the time it terminates. This does not provide continuous tracking and is far less geographically precise than the "virtual map of [a cell phone user's] movements" posited by the Federal Defenders. See

Statute, simply allows law enforcement to maintain a capability it has always had - the ability to locate a telephone user at the time a call is made or received on a prospective basis - in the face of changing technology. What is more, Section 2703(d) requires the Government to satisfy an "articulable facts" standard, an even higher burden than that required for a pen/trap order and which is in keeping with CALEA's increased privacy protections, discussed in Section B.3 below.

Finally, it is significant that Congress, in enacting CALEA following Director Freeh's testimony, did not ban the use of pen/trap orders to allow the disclosure of cell-site information from cellphone companies. Instead, it specified that such disclosure should not be made "solely pursuant" to a pen/trap order. 47 U.S.C. § 1002(a)(2)(B). The term "solely" is not wholly prohibitive. Rather, it is partially restrictive. This phrasing therefore implies that Congress in 1994 understood cell-site information to be covered by the Pen/Trap Statute. Indeed, if cell-site information could not be collected at that time pursuant to a pen/trap order, there would have been no need for Congress to limit such collection.

Challenging the Government's position on the combined authority of the SCA and the Pen/Trap Statute, the Magistrate Judges' opinions, as well as the Federal Defenders' brief, also raise questions about this combined authority's date of origin. See Texas Op. at *15; New York Op. at *25; Fed. Def. Br. at 19-20. This matter is not as mysterious as they suggest and, in any event, it has no bearing on the propriety of the Government's argument. As discussed above, the best answer is 1994: Director Freeh's testimony demonstrates that when Congress enacted CALEA in 1994 (with its "solely pursuant" language), it intended for cell-site information to be obtained pursuant to process under the SCA. In addition, as discussed above, CALEA's "solely pursuant" language suggests that Congress intended cell-site information to be covered by the Pen/Trap Statute.

Nevertheless, after CALEA was passed in 1994, some uncertainty remained over which categories of non-content information the Pen/Trap Statute covered. See Fighting Cyber Crime: Hearing Before the Subcommittee on Crime of the Committee

---

Fed. Def. Br. at 4. Indeed, it reveals considerably less information about a caller's location than the physical addresses associated with landlines under the "old" hardline system.

on the Judiciary, 107th Cong., 1st Sess. 47-48 (2001) (statement of Michael Chertoff, Assistant Attorney General, Criminal Division, U.S. Dep't of Justice) (available at judiciary.house.gov/legacy/chertoff_061201.htm). Any ambiguity was eliminated by the USA PATRIOT Act of 2001 § 216, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "Patriot Act"). As discussed in the Government's October 5 Letter at 7-8, disclosure of cell-site information now plainly falls within the definitions of "pen register" and "trap and trace device," and the Government is now clearly required to obtain such information using the Pen/Trap Statute and the SCA. This result is consistent with the result envisioned in 1994 by Congress and FBI Director Freeh: cell-site information is not available "solely pursuant" to a pen/trap order, but it is available when a Section 2703(d) order is used as well.

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

In its October 5 Letter, the Government explained that the combined authority of the Pen/Trap Statute and the SCA authorize courts to order the prospective disclosure of cell-site information. See October 5 Letter at 5-10. Magistrate Judges as well as the Federal Defenders, disagree. See Texas Op. at *13; New York Op. at *23; Fed. Def. Br. at 15-16. As explained below, however, their objections are without merit.

1. Cell-site Information Falls Within the Scope of the Pen/Trap Statute

As explained in the Government's October 5 Letter, pen registers and trap and trace devices, by definition, involve the disclosure of "dialing, routing, addressing, or signaling information" for outgoing and incoming telephone calls, respectively. See 18 U.S.C. §§ 3127(3) and (4); October 5 Letter at 7-8. Cell-site information tells a cellphone company with which cell tower a cellphone is in contact, thus allowing the cellphone company to provide service to the cellphone. Accordingly, cell-site information is used as signaling information to route cellphone calls, and the disclosure of this data falls squarely within the scope of the definitions for pen registers and trap and trace devices.

There are several reasons why the Magistrate Judges' contrary conclusion is incorrect. First, when Congress, via the Patriot Act in 2001, expanded the definition of pen registers and trap and trace devices to include "dialing, routing, addressing, or signaling information," it was not writing on a blank slate. In 2000, the Court of Appeals for the D.C. Circuit had already held that cell-site information was "signaling information" for purposes of CALEA. In United States Telecom Ass'n v. FCC, 227 F.3d 450 (D.C. Cir. 2000), the D.C. Circuit addressed whether cell-site information was "call-identifying information," which is defined by CALEA to mean "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." United States Telecom Ass'n v. FCC, 227 F.3d at 457 (citing 47 U.S.C. § 1001(2)). The court held that it was, explaining 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.'" Id. at 463 (internal quotations omitted). While noting that CALEA could have been clearer on its face, the D.C. Circuit observed that because cell-site information is signaling information, it fell within the type of information covered by the Pen/Trap Statute. Id. at 458, 463-64.

Moreover, once the Patriot Act expanded the statutory definition of pen register and trap and trace device to cover "signaling information," the Pen/Trap Statute's inclusion of cell-site location information became explicit. Indeed, this Court must presume that Congress was aware that cell-site information was signaling information when it enacted the Patriot Act. See Lorillard v. Pons, 434 U.S. 575, 580-81 (1978) ("Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change. . . . So too, where, as here, Congress adopts a new law incorporating sections of a prior law, Congress normally can be presumed to have had knowledge of the interpretation given to the incorporated law, at least insofar as it affects the new statute.").

Second, whose arguments Magistrate and the Federal Defenders in large part repeat, erroneously constrains the Patriot Act's expansion of the pen/trap definitions to reach only the Internet. See Texas Op.

RIP

at *13; New York Op. at *23; Fed. Def. Br. at 13-16. In support, (7C) points to two statements in the Congressional Record noting that the expanded definition of pen register and trap and trace device will apply to the Internet. See Texas Op. at *13. Yet contrary to (7C) conclusion, nothing in these two statements indicates that the expanded definitions are restricted only to the Internet. Moreover, not only is (7C) inference foreclosed by the D.C. Circuit's holding in United States Ass'n v. FCC that cell-site information is "signaling information" (and thus falls within the scope of the expanded definitions of pen registers and trap and trace devices), but it is also inconsistent with the Patriot Act's statutory language and legislative history. Nothing in the definition of pen register and trap and trace device limits those terms to a particular method of communications, be it the Internet, cellphones, or hardline telecommunications. See 18 U.S.C. §§ 3127(3) and (4). In fact, none of the electronic surveillance statutes - 18 U.S.C. § 2510, et seq. (the "Wiretap Act"), the SCA, and the Pen/Trap Statute - apply only to particular communications technologies. They are written in technology-neutral terms, and thus apply equally to all network and communications technologies. As the House Report on the Patriot Act explained: "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." H.R. Rep. No. 236(I), 107th Cong., 1st Sess. at 53 (2001) (emphasis added).

Third, (7C) and the Federal Defenders argue that the Pen/Trap Statute does not cover cell-site information because such information is not "generated by, and incidental to, the transmission of 'a wire or electronic communication.'" Texas Op. at 13 & n.19. See also Fed. Def. Br. at 16. Their argument, however, relies in part on their insistence that cell-site information constitutes tracking information insufficiently tied to the telephone calls themselves. See Section C below. By definition, however, a pen register records information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). Because cellphone voice communications are wire communications, see 18 U.S.C. § 2510(1), there can be no dispute that a cellular telephone network is a facility from which a wire communication is transmitted. Similarly, a trap and trace device collects "dialing, routing, addressing and signaling information reasonably likely to identify the source of a wire or electronic communication," 18

RIP 7C

U.S.C. § 3127(4), and cell-site information is used to identify the source of a wire communication (a cellphone call). In other words, the pen registers and trap and trace devices are defined by the "instrument," "facility" or "source" from which they collect information, not whether the information itself must be tied to an electronic or wire communication. (7C) (7C) declined to rely on (7C) on this point, commenting that "as I read the amended definition [of pen registers and trap and trace devices], it merely ties the concept of 'wire or electronic communication' to the 'instrument or facility' to which the pen register relates." See New York Op. at *23. Accordingly, cell-site information plainly falls within the definitions of pen registers and trap and trace devices and is subject to the Pen/Trap Statute.

Finally, to exclude cell-site information from the Pen/Trap Statute, (7C) relies in part on the fact that separate frequencies may be used to transmit voice information and information relating to cell-site location. See Texas Op. at *2-*3. This distinction, however, is irrelevant under the language of the Pen/Trap Statute and the SCA. Cell-site information, no matter by which channel it travels, remains signaling information transmitted by a facility from which a wire communication is transmitted, and it is still a record pertaining to a customer of an electronic communication service.

For its part, the Federal Defenders' brief argues that cell-site information falls outside of the scope of pen registers and trap and trace devices because they only address "basic" information, while the Government seeks "detailed" cell-site data. See Fed. Def. Br. at 15. Indeed, the Federal Defenders' brief attempts to make much of the fact that certain technologies may allow for greater precision in the tracking of cellular telephones, declaring that it would create a "virtual map of [a cellphone user's] movements". Id. at 2-4. This is not, however, the type of information that the United States Attorney's Office for the Southern District of New York has for several years successfully sought in its standard applications for cell-site orders (a sample of which was attached to its October 5 Letter). Here, this Office seeks data which comports with the so-called "J-Standard," that is, cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from a particular cellphone. See United States Telecom Ass'n v. FCC, 227 F.3d at 455. Notably, this is a much smaller set of information than the Government sought in the case before (7C)

RIP
7C

(where the Government also sought cell-site information during the progress of the call), see New York Op. at 1, and the case before (7C) (where the Government also sought "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites."), see Texas Op. at 1. As explained in the Government's October 5 Letter, the cell-site information sought by this Office, at best, shows the cell quadrant a cellphone was in.[2] See October 5 Letter at 1. It is not the "host" of information that Federal Defenders alleges would fall into an "altogether different category" than other information collected by pen registers and trap and trace devices.[3] In any event, there is nothing in the Pen/Trap statute that requires the information collected to be "basic" versus "complex." Rather, the distinction to be drawn is "content" as opposed to "non-content" and whether the information is "dialing, routing, addressing, and signaling information." As discussed above, cell-site information is at least signaling information. Finally, as discussed in Section A above, the prospective disclosure of J-Standard cell-site information merely maintains the same surveillance capability that existed before the introduction of cellphones as mandated by CALEA.

2. Cell-Site Information Falls Within the Scope of the SCA

Section 2703(c)(1) of the SCA requires "a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service" pursuant to a 2703(d) order. 18 U.S.C. § 2703(c)(1). See also October 5 Letter at 5-6. A cellphone company is a provider of electronic communication service because it provides its users with the ability to send or receive wire or electronic communications. See 18 U.S.C. § 2510(15). Moreover, as the Government explained in its October 5 Letter, cell-site information is "a record or other information pertaining to a subscriber or customer of such service." October 5 Letter at 5.

---

[2] While the Government believes the larger set of information does not make a cellphone a tracking device, that issue is not presented here.

[3] In fact, the Federal Defenders concedes that "society may be willing to accept the idea of collecting information associated with the origination and termination of calls." See Fed. Def. Br. at 24 (internal quotes and citation omitted).

RIP 7C

Accordingly, disclosure of cell-site information may be obtained pursuant to 18 U.S.C. §§ 2703(c)(1) and (d). Id. at 5-6.

However, concludes that cell-site data does not fall within the scope of the SCA based on his categorization of cellphones as "tracking devices" - the same reason he relied on to support his conclusion that the Pen/Trap Statute did not apply to cell site data. Specifically, first asserts that the issue under Section 2703(c)(1) is whether prospective cell-site data "may constitute a record pertaining to 'wire or electronic communications,'" and then claims that cell-site information is not a wire or electronic communication because its disclosure would render cellphones as "tracking devices." Texas Op. at *10-*11. and the Federal Defenders follow reasoning to reach the same conclusion. See New York Op. at *12-*14; Fed. Def. Br. at 6-8. This is error. As discussed in Section C below, disclosure of cell-site data does not implicate the tracking device statute. Moreover, initial premise is grounded in a misreading of the statute. Section 2703(c)(1) governs records pertaining to a subscriber or customer of an "electronic communication service," such as a cellphone company, not - as would have it - records specifically pertaining to wire or electronic communications. For example, a cellphone company's customers' names, addresses, and detailed billing information are records pertaining to customers of an electronic communication service, but they are not records pertaining to wire or electronic communications. See Jessup-Morgan v. America Online, Inc., 20 F. Supp.2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer's identification information is a "record or other information pertaining to a subscriber"). To the same extent, cell-site information is a record pertaining to a subscriber or customer of an electronic communication service. See October 5 Letter at 5. In other words, the question is whether that information concerns a subscriber or customer of an electronic communications service; it makes no difference whether these data ultimately pertain to a wire or electronic communication.

The weakness of argument that cell-site information does not fall within the scope of Section 2703(c)(1) is further illustrated by his admission that Section 2703(c)(1) includes historical cell-site data. See Texas Op. at *11 n.16. See also New York Op. at *31; Fed. Def. Br. at 12. Based on the language of Section 2703(c)(1), however, there is no

reason to distinguish historical from prospective cell-site data when determining whether such information is "a record or other information pertaining to a subscriber or customer." A court may not pick and choose when cell-site information will constitute "a record or other information pertaining to a subscriber or customer" of an electronic communication service. For this reason, too, (7C) claim that cell-site information does not fall within the scope of the SCA must fail.[4]

3. The Privacy Provisions of CALEA Substantively Changed Electronic Surveillance Law

The Magistrate Judges' opinions also reject the Government's argument that the combined authority of the Pen/Trap Statute and the SCA allows for the prospective disclosure of cell-site information, reasoning that CALEA did not amend existing surveillance law when it forbade the disclosure of location information "solely pursuant" to a pen/trap order. See Texas Op. at *13; New York Op. at *24. In effect, they argue that since CALEA did not change the substantive law of electronic surveillance, its "solely pursuant" limitation has no real significance.

CALEA's statutory language and legislative history demonstrate otherwise. While one purpose of CALEA "was to allow law enforcement to retain existing surveillance capabilities in the face of technological change," Texas Op. at 25, there were other aims as well.[5]

---

[4] (7C) raises one additional issue regarding the Government's authority under the SCA. He states, correctly, that an order under Section 2703 can only compel disclosure by a provider. See New York Op. at *18. That is precisely what the Government seeks through the combined authority of the Pen/Trap Statute and the SCA - cell-site location information from the cellphone company.

[5] CALEA ensured that law enforcement's existing surveillance capabilities would be preserved by requiring telecommunications companies to maintain certain technical capabilities, such as the ability to "isolate expeditiously the content of targeted communications." See H.R. Rep. No. 103-827, at 9-10 (1994), reprinted in 1994 U.S.C.C.A.N. 3489. The "J-Standard," discussed above at 5 n.1, "outline[d] the technical features, specifications, and protocols for carriers to make

RIP
7C

Notably, CALEA substantively changed the electronic surveillance statutes to enhance privacy, and did so in two principal ways. First, it created the 2703(d) "articulable facts" order for transactional information associated with electronic communications. Up to that time, such records had been available merely pursuant to a subpoena. See CALEA § 207, P.L. 103-313, 108 Stat. 4279, 4292 (1994). Second, it forbade disclosure of cell-site information by a provider "solely pursuant" to a pen/trap order. See CALEA § 207, P.L. 103-313, 108 Stat. 4279, 4280-81 (1994). CALEA's legislative history even explicitly states that the latter restriction on pen/trap orders was a substantive change in the law intended to enhance privacy. In a section entitled "The Legislation Addresses Privacy Concerns," the House Report on CALEA states:

> [T]he bill . . . [e]xpressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information.

See H.R. Rep. No. 103-827, at 17 (1994), reprinted in 1994 U.S.C.C.A.N. 3497 (emphasis added). Significantly, this portion of the House Report demonstrates both that Congress intended CALEA to amend the substantive rules of surveillance law and that Congress understood that prior to CALEA, cell-site information had been available pursuant to a pen/trap order. See also United States Telecom Ass'n v. FCC, 227 F.3d at 463-64.

Against this statutory background, the Magistrate Judges' opinions claim that CALEA's "disclaimer of pen/trap authority was intended to assure that the existing legal framework would continue to apply in spite of anticipated legal advances" is erroneous. See Texas Op. at *15 (emphasis in original); New York Op. at *24. The Magistrate Judges' opinions fail to distinguish between the technological mandates of CALEA, which did not modify the statutory framework for electronic surveillance, with the privacy-enhancing features of CALEA, which did change that

---

subscriber communications and call-identifying information available to law enforcement agencies having appropriate legal authorization." United States Telecom Ass'n v. FCC, 227 F.3d at 455.

framework. For example, when the opinions cite FBI Director Freeh's statement that CALEA "relates solely to advanced technology, not legal authority or privacy," Texas Op. at *14; New York Op. at *24, they fail to realize that Director Freeh was testifying early in the legislative process, prior to the addition of CALEA's privacy-enhancing features. Section 2703(d) "articulable facts" orders are not mentioned in Director Freeh's testimony because they were not yet part of the bill. See also supra at 4. Indeed, as noted above, it was Director Freeh himself who first proposed the restriction on disclosure of cell-site information solely pursuant to a pen/trap order. See supra at 3-4.

Finally, argument that CALEA's changes were non-substantive violates the fundamental canon of statutory construction that a court should give effect to each statutory provision. See Washington Market Co. v. Hoffman, 101 U.S. (11 Otto) 112, 115-16 (1879). If CALEA's language limiting disclosure of cell-site information "solely pursuant" to a pen/trap order did not change electronic surveillance law, what, then, did it do? The Magistrate Judges' opinions hold that CALEA "relates solely to advanced technology, not legal authority or privacy." Texas Op. at *13; New York Op. at *24. While that may have been true with respect to the draft of CALEA initially introduced, it was not the case with respect to CALEA as it was ultimately enacted. As noted above, Director Freeh's testimony played a significant role in spurring additions to CALEA. The pen/trap "solely pursuant" restriction changed the substantive law of pen/trap orders to enhance privacy, by requiring the Government to seek prospective cell-site information pursuant to the dual authority of the Pen/Trap Statute and the SCA with its articulable facts requirement. Significantly, neither the Magistrate Judges' opinions nor the Federal Defenders brief explain what effect the "solely pursuant" language could have other than the one set forth by the Government.

4. Prospective Disclosure of Cell-Site Information Is Authorized By the SCA

Prospective disclosure of cell-site information falls within the scope of the SCA. As discussed previously, cell-site data are "record[s] or other information pertaining to a subscriber or customer" under Section 2703(c) of the SCA. The SCA does not impose any temporal restriction in either its description of "records or other information" or its procedures for disclosing

RIP

that information. Thus, nothing within the SCA prevents disclosure of cell-site information on a prospective basis. Historical and prospective data are not treated differently, and courts should not engraft such a limitation onto the SCA where Congress has not done so.

Nonetheless, the Magistrate Judges' opinions insist on bifurcating "records and other information" into past and future time zones. See supra at 12-13. Lacking any support in the SCA itself for this split, the Magistrate Judges' reasoning instead depends, once again, on the categorization of cellphones as "tracking devices." As discussed in Section C below, this is an erroneous designation. Curiously, (7C) also places historical cell-site data in the category of "transactional records" covered by the SCA, but takes prospective cell-site data out of that category altogether. See Texas Op. at *11 n.16. This is a wholly artificial construct.

Lacking any textual support in the SCA for their historical/prospective bifurcation, the Magistrate Judges' opinions instead seize upon the lack of procedural features in the SCA as evidence that is was not meant to apply prospectively. See Texas Op. at *11-*12; New York Op. at *13. See also Fed. Def. Br. at 12-13. For example, the SCA includes no duration requirement and no sealing requirement. Contrary to the assertions of (7C) however, there is simply no reason for the SCA to contain such procedural elements. Prospective disclosure of cell-site information is governed by both the SCA and the Pen/Trap Statute. Thus, when the SCA is used prospectively to gather cell-site information, the collection is also governed by the Pen/Trap Statute, and all the procedural features of that law apply to the government's subsequent collection of cell-site data. In practice, prospective applications and orders for cell-site information should satisfy the requirements of both the pen/trap statute and the SCA. As discussed in Section A above, this is the result Congress intended when it enacted the pen/trap restriction of CALEA, because it understood that the disclosure of cell-site information would continue only pursuant to the heightened "articulable facts" standard of Section 2703(d) orders. This dual-authority requirement thus creates a regime in which pen/trap orders for cell-site information may be issued, but only when the Government also satisfies an "articulable facts" evidentiary showing.

RIP
7C

In his analysis, (7C) further suggests that prospective use of the SCA would enable the Government to bypass the restrictions of the Wiretap Act. See New York Op. at *18. That is untrue. Prospective use of the SCA to allow for the disclosure of content would violate the Wiretap Acts's prohibition on interception of wire or electronic communications. See 18 U.S.C. § 2511. Both the Wiretap Act and the Pen/Trap Statute include strict mandates on prospective disclosure of content and non-content information, respectively. The Government cannot intercept communications without complying with the Wiretap Act, and it cannot acquire pen/trap data, like cell-site information, without complying with the Pen/Trap Statute. The congressional requirement that the Government cannot seek the disclosure of cell-site information "solely pursuant" to a pen/trap order requires the Government to also rely on the SCA for such disclosure, but it does not allow an end-run around either the Pen/Trap Statute or the Wiretap Act.

C. **The Tracking Device Statute Is Not Relevant to Orders for the Prospective Disclosure of Cell-Site Data**

In its October 5 Letter, the Government explained in detail why a cellphone is not a "tracking device." See October 5 Letter at 12-13.[6] Rather than repeat in full that explanation here, the Government instead will focus on responding to the points set forth in the Magistrate Judges' opinions and the Federal Defenders' brief.[7]

---

[6] Indeed, Director Freeh distinguishes cell-site orders, which provide "generalized location information" from tracking devices, which provide more specific location data, in his testimony before Congress in connection with CALEA. See Freeh Testimony, 1994 WL 223962 at *27-28. Furthermore, as discussed above, the United States Attorney's Office for the Southern District of New York in this case seeks a smaller set of cell-site information than the applications in the cases before (7C) Thus, it is even more difficult in this case than in those cases to claim that the disclosure of cell-site information amounts to a "tracking device" within the meaning of Section 3117(b).

[7] Some of these points have already been addressed above. In Section B.1, the Government explained why cell-site information is subject to the Pen/Trap statute regardless of whether a cellphone is tracking device. Similarly, in Section

REP
7C

Section 3117, notes, is a short statute with a limited purpose. See Texas Op. at *3. It specifies only 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." 18 U.S.C. § 3117(a). By its terms, then, the statute has a very restricted purpose: to provide a court authority in certain circumstances to authorize use of a tracking device which may be used outside of the court's jurisdiction. This narrow purpose is the only one discussed in the legislative history of the Electronic Communications Privacy Act ("ECPA"), § 108, Pub. L. No. 99-508, 100 Stat. 1848 (1986), the act which enabled the tracking device statute. See S. Rep. No. 99-541 at 33-34 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3587-88. In addition, in order to make clear that use of a tracking device does not require a wiretap order, the definition of "electronic communication" excepts "any communication from a tracking device." 18 U.S.C. § 2510(12)(B).

From this limited procedural statute, the Magistrate Judges' opinions develop a separate tier of electronic surveillance law. They place the tracking device statute on a par with the Wiretap Act, the SCA, and the Pen/Trap Statute, which characterizes as the "four broad categories" of electronic surveillance law.[8] See Texas Op. at *4-*5. But the tracking device statute will not bear the weight they seek to place on it. Their categorization rests on the premise that tracking devices require a warrant based on probable cause. See id. at *3-*5; New York Op. at *26-*27. This premise, however, is incorrect. The tracking device statute does not require the Government to seek a warrant based on probable cause when using a tracking device; indeed, the statute does not even prohibit the use of a tracking device in the absence of conformity with Section 3117. See United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000). Even when the Government invokes the limited authority provided

---

B.2, the Government explained why cell-site information falls within the scope of Section 2703(c)(1) regardless of whether a cellphone is a tracking device.

[8] Indeed, all of the arguments in the Magistrate Judges' opinions and the Federal Defenders' brief essentially rely on the argument that the prospective disclosure of cell-site information converts cellphones into "tracking devices."

by the tracking device statute, it does not require a search warrant. Rather, it requires only that the court be empowered to issue "a warrant or other order" for the tracking device. 18 U.S.C. 3117(a). Finally, the tracking device statute applies only where the court has ordered "installation" of a tracking device. Id. When seeking disclosure of cell-site information from a cellphone company, the Government is not seeking to install anything. Accordingly, nothing in the tracking device statute limits the Government's ability to obtain cell-site information pursuant to the Pen/Trap Statute and the SCA.

In addition, ECPA's drafters understood that there was no constitutional warrant requirement for tracking devices that do not violate a reasonable expectation of privacy. For example, the House Report on ECPA discusses United States v. Knotts, 460 U.S. 276, 285 (1983) (upholding warrantless use of beeper to track vehicle on public roads) and United States v. Karo, 468 U.S. 705, 713-18 (1984) (holding that warrantless use of beeper inside a house violated the Fourth Amendment), and it notes that Section 3117 "does not affect the legal standard for the issuance of orders authorizing the installation of each device." H.R. Rep. No. 647, 99th Cong., 2d Sess., at 60 (1986). See also Texas Op. at *3. ("The ECPA was not intended to affect the legal standard for the issuance of orders authorizing [tracking devices].") Therefore, Congress was quite clear that it was not imposing a statutory warrant requirement on the use of statutorily defined tracking devices, and the courts should not impose such a requirement where Congress has not done so. [9]

---

[9] ( ) also contends that even the mere possibility that a tracking device could disclose information relating to a private space is sufficient to require the Government to seek a warrant based on probable cause. See Texas Op. at *9. ( ) and the Federal Defenders adopt this reasoning. New York Op. at *28; Fed. Def. Br. at 22-23. This view is error in light of Karo, where the Supreme Court specifically reserved this question. In Karo, the Supreme Court stated: "The United States insists that if beeper monitoring is deemed a search, a showing of reasonable suspicion rather than probable cause should suffice for its execution. That issue, however, is not before us. The initial warrant was not invalidated for want of probable cause, which plainly existed, but for misleading statements in the affidavit. . . . It will be time enough to resolve the probable cause-reasonable suspicion issue in a case that requires it." United States v. Karo, 468

Further, by its own terms, the definition of "tracking device" given in Section 3117 is limited to devices installed pursuant to a court order. See 18 U.S.C. § 3117(b). This is significant because it plainly excludes any device that an individual voluntarily carries and uses, such as Blackberries, text-based beepers, and cellphones.

Finally, a consequence of analysis would be to eviscerate privacy protection for millions of users of Blackberries or text-based pagers which rely on cellphone networks. If a Blackberry or a pager were a tracking device for purposes of Section 3117 - and it would be under statutory interpretation - it could not be used to send an electronic communication, because the definition of "electronic communication" excludes "any communication from a tracking device." 18 U.S.C. § 2510(12)(B). Consequently, there would be nothing to prevent private individuals from intercepting communications from such devices without violating the Wiretap Act.[10] attempts to avoid this necessary consequence of his argument by suggesting that cellphones are sometimes tracking devices and sometimes not, depending on the type of cellphone communication being monitored. See Texas Op. at *2-*3, *7. However, the language of the tracking device statute does not support such parsing. The tracking device statute depends on installation pursuant to a court order. Thus, any user-owned and carried device cannot fall within the ambit of the tracking device statute.

further suggests that the Government "threatens to undermine the federal statutory scheme for electronic surveillance" by surreptitiously installing cellphones instead of traditional beeper devices. See Texas Op. at *8. This assertion is meritless. As an initial matter, the law

---

U.S. at 718 n.5. However, because there is no reasonable expectation of privacy in cell-site information, as discussed below, this case does not require resolution of this issue. Moreover, the generalized, "J-Standard" cell-site data sought by the Government - not the "virtual map of a [cellphone user's] movements" as claimed by the Federal Defenders - would not provide sufficiently localized information such that private spaces would be invaded.

[10] Cellphone communications containing the human voice will remain protected as wire communications.

RIP

governing the use of beepers is based on the Fourth Amendment, not a "federal statutory scheme." Indeed, as the D.C. Circuit noted in Gbemisola, the tracking device statute does not prohibit the use of a tracking device in the absence of conformity with Section 3117. See United States v. Gbemisola, 225 F.3d at 758 ("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). Furthermore, if the Government were installing the cellphone, the dictates of the tracking device might very well apply. More significantly, there is no dispute that if the Government surreptitiously installs a cellphone in an item given to a target, the Government's monitoring of the cellphone would be judged under the constitutional framework set forth by the Supreme Court in United States v. Knotts, 460 U.S. 276, 285 (1983), and United States v. Karo, 468 U.S. 705, 713-18 (1984). Here, however, the Government merely seeks disclosure of information conveyed by a voluntarily possessed and used cellphone to a third-party cellphone company. As discussed below in Section D, there is no reasonable expectation of privacy in such information and, accordingly, no Fourth Amendment privacy concerns are implicated.

D. There Is No Reasonable Expectation of Privacy in Cell-Site Information

In order to receive service from a cellphone company, the owner of a cellphone must transmit a signal to a nearby cell tower to register his or her presence within the network. Cellphone companies keep track of such information in a database, something they must do to complete calls to and from the cellphone. Under the established principles of Smith v. Maryland, 442 U.S. 735 (1979), there can be no reasonable expectation of privacy in such information. See October 5 Letter at 11-12. (7C) followed by (7C) and the Federal Defenders, dispute this conclusion. See Texas Op. at *8; New York Op. at *27-*28; Fed. Def. Br. at 23-24. Their position, however, is erroneous.

The Smith case is controlling here. The Smith Court held both that telephone users had no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. See Smith, 442 U.S. at 742-44. The Court's reasoning also applies to cell-site information. First, the Court stated: "we doubt that people in general entertain any

RIP
7C

actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." Smith, 442 U.S. at 742. This logic also holds for cellphones: cellphone users understand that they are broadcasting a signal to the cellphone company so that the cellphone company can locate them to complete their calls.

Moreover, under the reasoning of Smith, any subjective expectation of privacy in cell-site information is unreasonable. In Smith, the Court explicitly held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable." Smith, 442 U.S. at 743 (internal quotation marks 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 dispositive here. A cellphone user must transmit a signal to the cellphone company and thereby assumes the risk that the cellphone provider will reveal the cell-site information to law enforcement. In other words, it makes no difference if some users have never thought about how their cellphones work or if they believe that the cellphone company locates them through magic. A cellphone user can have no expectation of privacy in cell-site information.

is simply mistaken when he asserts that cell-site date is not voluntarily conveyed by the user, or that it is transmitted "independent of the user's input, control or knowledge." Texas Op. at *8. The process of turning on a cellphone is a voluntary act, as is the process of sending or receiving a cell call. It is true that if someone wants to use a cellphone, he or she must turn it on and send a signal to the cellphone company. But such an action is no more involuntary than dialing a number to make a telephone call. If someone wants to make a phone call, he or she must reveal the phone number to the telephone company. To the same extent, if someone wants to use a cellphone, he or she must send a signal to the cellphone company, and the company will receive the signal at a particular cell tower. See United States Telecom Ass'n v. FCC, 227 F.3d at 459 (stating that "Smith's reason for finding no legitimate

expectation of privacy in dialed telephone numbers - that callers voluntarily convey this information to the phone company in order to complete calls - applies as well to much of the information provided by the challenged capabilities," which included the ability to disclose cell-site information).

Indeed, when purchasing a cellphone or subscribing to cellphone service, most cellphone users are well aware that they will be signaling their location to the cellphone company when they are using their cellphone. The type and cost of service is typically tied to the location of the user. In fact, cellphone customers are usually given maps outlining their calling plan's geographical boundaries, and ubiquitous "roaming fees" are charged if calls are made from outside these areas.

The Supreme Court decisions in Knotts and Karo are plainly inapplicable to the disclosure of cell-site information. Smith is controlling in this case for a simple and fundamental reason: Knotts and Karo involved surreptitious installation by the Government of a transponder, whereas Smith and this case involve the disclosure of information in the possession of a third party. Further, even under the standard of Knotts and Karo, there is no reasonable expectation of privacy in cell-site information. In Knotts, the Supreme Court held that law enforcement monitoring of a beeper along public highways did not violate the Fourth Amendment. United States v. Knotts, 460 U.S. 276, 282 (1983). In Karo, the Court held that police monitoring of a beeper which disclosed information about the interior of a house, not open to visual surveillance, does implicate Fourth Amendment privacy interests. United States v. Karo, 468 U.S. 705, 713 (1984). "J-standard" cell-site information, however, is not sufficiently particularized to pinpoint the location of a cellphone in a private space, and the Fourth Amendment protects only such specific location information. In Karo, when law enforcement used a beeper to locate a container of ether in a warehouse, it did not use the beeper to identify the specific locker containing the targeted ether - that was done by smell from a public part of the warehouse. United States v. Karo, 468 U.S. at 720-21. The Supreme Court found no constitutional violation, explaining that "[h]ad the monitoring disclosed the presence of the container within a particular locker the result would be otherwise, for surely [the defendants] had a reasonable expectation of privacy in their own storage locker." Id. at 720 n.6. Thus, law enforcement does not violate the Fourth Amendment when it uses a beeper to determine the general location of an object, even if there is a reasonable expectation of privacy in the object's specific location. Under this reasoning, the generalized

location information available from cell-site data does not implicate Fourth Amendment privacy concerns.

Moreover, as previously noted by the Government, see October 5 Letter at 12, the privacy interest of a target in cell-site information is even less than the privacy interest in dialed telephone numbers. Cell-site information is generated internally by the service provider - a customer will not even know where the cell towers are. It would be entirely unprecedented in Fourth Amendment jurisprudence to find that a defendant has a reasonable expectation of privacy in information he or she does not know about and has not ever possessed. It is true, as 7C notes, that United States v. Forest, 355 F.3d 942, 951-52 (6th Cir. 2004), rejects the application of Smith to cell-site information, holding that it is not voluntarily conveyed by cellphone users because it is transmitted automatically or may be triggered by law enforcement dialing the cellphone. Texas Op. at *8. However, Forest's discussion of this issue is dicta because the court in Forest held that the defendants had no reasonable expectation of privacy under the principles of Knotts and Karo. In any case, Forest's dicta is incorrect for the reasons explained above; that is, the court failed to understand that cellphone users have no legitimate expectation of privacy in the cell-site location information conveyed to their cellphone company.

Finally, 7C reliance on the Wireless Communication and Public Safety Act of 1999 (the "WCPSA") is similarly misplaced. 7C asserts that the WCPSA demonstrates that "location information is a special class of customer information, which can only be used or disclosed by a carrier in an emergency situation, absent express prior consent by the customer." Texas Op. at *9. This assertion is incorrect. In fact, the WCPSA states that "[e]xcept as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose or permit access to individually identifiable customer proprietary network information" in certain specified situations. 47 U.S.C. 222(c)(1) (emphasis added). The phrase "except as required by law" encompasses appropriate criminal legal process. See Parastino v. Conestoga Tel. & Tel. Co., No. Civ. A 99-697, 1999 WL 636664, at *1-*2 (E.D. Pa., Aug. 18, 1999) (holding that a valid subpoena falls within the "except as required by law" exception of § 222(c)(1)). Such criminal process includes process under the SCA. 7C quotes Section 222(f) of the WCPSA, see Texas Op. at *8-*9, but this

RIP
7C

provision does not limit the "as required by law" exception. Instead, Section 222(f) sets rules for determining whether a customer has consented to voluntary disclosure of his cell-site information. Thus, the WCPSA does not in any way limit the disclosure of cell-site information pursuant to the SCA. Furthermore, the fact that Congress has provided additional statutory protections of cell-site information does not create a constitutional reasonable expectation of privacy in that information. For example, the pen/trap statute and the SCA create statutory privacy rights in dialed phone numbers, but dialed phone numbers remain constitutionally unprotected under Smith v. Maryland.

CONCLUSION

For the reasons stated above, the Government respectfully submits that the Court has authority, pursuant to the Pen/Trap Statute and the SCA, to order the prospective disclosure of cell-site information.

Respectfully submitted,

MICHAEL J. GARCIA
United States Attorney

By: _____
Assistant United States Attorney

cc: Federal Defenders of New York, Inc.
(By Hand)