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

(TC) 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 (TC) 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
TC

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