

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AN ORDER AUTHORIZING THE DISCLOSURE
OF PROSPECTIVE CELL SITE INFORMATION

06 MISC. 004

Application No. 5485

DECISION AND ORDER

On December 23, 2005, the government filed with this court, under seal, an application for an order authorizing the disclosure of prospective cell site information exclusively pursuant to 18 U.S.C. §§ 2703 and 3122. Specifically, the government seeks an order requiring Cingular Wireless, and any other providers of electronic communication service whose assistance is needed to comply with the order, to disclose to agents of the Wisconsin Department of Justice, Division of Criminal Investigation, certain information for a particular cellular telephone for a period of sixty days (60) from the date the order is signed. The information being sought is the following:

- a. Originating and terminating cellular tower and sector information for all calls to and from this cellular telephone (i.e., cell site activations);
- b. Map of cellular tower locations/addresses, sectors and orientations; and
- c. The physical address/location of all cellular towers in the applicable markets.

In support of its application, the government presents, *inter alia*, that "[a]gents from DCI [the Wisconsin Department of Justice, Division of Criminal Investigation, Narcotics Bureau] believe that by obtaining cell-site information for [the subject's] cellular telephone, it may be able to determine [the subject's] source for cocaine." (App. at 3.) Thus, the government "requests that the Court issue an order authorizing the use of the pen register device which has been authorized in [previous

applications] to also record and disclose signaling information, including cell site information, from the target telephone for incoming and outgoing calls for a period of sixty (60) days from the date of this order." (App. at 4.) What makes this particular application a bit problematic is the prospective nature of the information being sought. In other words, the information being sought is not "historical information." Whether the government has the statutory right¹ to seek such information has been the subject of a number of recent decisions.

At least three courts have decided that there is no statutory authority to support the government's request. See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (the "Southern Texas Case" or "Southern Texas"); In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (the "EDNY Case" or "EDNY"); and In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and the Production of Real Time Cell Site Information, 2005 WL 3160860 (D. Md. Nov. 29, 2005) (the "Maryland Case" or "Maryland").

More recently, however, in *In re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 2005 WL 3471754 (S.D.N.Y. December 20, 2005) (the "SDNY Case" or "SDNY"), the

¹ The government's application is predicated only on the combined authority of 18 U.S.C. §§ 2703 and 3122. In seeking issuance of the order, the government has made no effort to satisfy the probable cause requirements of Fed. R. Crim. P. 41. Thus, the question of whether a search warrant issued in accordance with the provisions of Rule 41 would support issuance of the requested order (if the appropriate showing were made) is not before me.

court granted the government's application for cell site information for a period of sixty days going forward from the date of the order.

In light of the somewhat unsettled status of the case law, I ordered the government to file a brief in support of its application. In accordance with that order, the government filed a brief setting forth its position regarding the statutory authority supporting its application. I have now considered the government's argument and the case law dealing with the issue. For the following reasons, the government's application will be denied.

By way of background, cellular telephone networks function by dividing a geographic area into many coverage areas, or "cells." Each cell contains 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. This information 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.

The government's application seeks the above-listed information ("prospective cell site information") for a cell phone assigned a specific mobile identification number for a period 60 days from the date of the order. The government seeks the order 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"). The government argues that

[t]he 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). However, 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 Pen/Trap Statute by itself is insufficient authority for such disclosure. 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.

(Gov't's Mem. at 7-8.)

In sum, it is the government's position that 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(b)(2). In turn, disclosure of cell site information requires a further demonstration by a 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). Because its application satisfies the combined requirements of sections 3122 and 2703(d), the government maintains that the order calling for the disclosure of prospective cell site information should be granted.²

As stated previously, the field of judicial decision on the question before this court is not entirely unplowed. At least four courts have spoken to the issue of whether the combined authority

² The government's argument has been referred to as the "hybrid" authority argument. *See Southern Texas*, 396 F. Supp. 2d at 761.

of §§ 3122 and 2703(d) provides a statutory basis to support the issuance of an order similar to that which the government seeks from this court. I say "similar" to that which the government seeks from this court because the information sought in the instant case is less extensive than the information sought by the government in both *Southern Texas* and *EDNY*. More specifically, in *Southern Texas* the government sought not only the information being sought here, but also sought information "regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites." 396 F. Supp. 2d at 749. In *EDNY*, the government was also seeking cell site information during the progress of a call. Furthermore, the court in *EDNY* determined that the government was also seeking to "obtain cell site information directly from its own devices and processes, rather than via disclosure from the telecommunications providers." 396 F. Supp. 2d at 314.

By contrast, the information being sought by the government in the instant case is more akin to that which was being sought in *SDNY*. Specifically, in *SDNY* the government indicated that it sought 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." *SDNY*, at *1. Such is the case here as well. Indeed, in its memorandum the government asserts that

[i]n the instant case and in the application before Judge Gorenstein in the Southern District of New York, the U.S. Attorney's Office is seeking 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. . . . [T]he cell-site information sought by this Office, at best, shows the cell quadrant a cellphone was in.

(Gov't's Mem. at 19-20.)

Be that as it may, the legal question before this court, at its heart, is the same legal question that was presented to the other four courts: does the combined application of 18 U.S.C. § 3122 and

18 U.S.C. § 2703(d) grant this court the statutory authority to order the disclosure of prospective cell site information of the type being sought by the government?

My analysis in this case begins with a review of the statutes that the issue presented has called into play. The first is the Pen/Trap Statute, 18 U.S.C. § 3121, et seq.

Title 18 U.S.C. § 3127(3) defines the term "pen register" as

any 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, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

In turn, 18 U.S.C. § 3121(a) provides, in pertinent part, that "[e]xcept as provided in this section, no person may install or use a pen register or trap and trace device without first obtaining a court order under section 3123 of this title." In order to obtain the court order called for in section 3123, the government must file an application with the court which includes

- (1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and
- (2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

18 U.S.C. § 3122(b)(1) and (2).

The second statute is the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, et seq. That statute sets forth, inter alia, the mechanism by which a provider of electronic communication service can be required to disclose to a governmental entity records or other information pertaining to a subscriber to, or customer of, such service (but not including the contents of communications).

See 18 U.S.C. § 2703(c). Certain subscriber or customer records/information can be obtained merely by using an administrative subpoena, grand jury subpoena or trial subpoena. See 18 U.S.C. § 2703(c)(2). However, in order to obtain records or information other than those records or that information listed in § 2703(c)(2) (but for purposes of this discussion, still not including the contents of communications), the government must: (1) obtain a warrant pursuant to the Federal Rules of Criminal Procedure (§ 2703(c)(1)(A)); (2) obtain a court order under subsection (d) of section 2703 (§ 2703(c)(1)(B)); (3) obtain the consent of the subscriber/customer (§ 2703(c)(1)(C)); or (4) submit "a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber of customer is engaged in telemarketing." 18 U.S.C. § 2703(c)(1)(D).

Section 2703(d) sets forth the requirements for the issuance of the court order referenced in section 2703(c)(1)(B). Section 2703(d) reads, in pertinent part, as follows:

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

18 U.S.C. § 2703(d).

Finally, there is the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), 47 U.S.C. § 1001, et seq. That statute requires telecommunications carriers to ensure that their equipment is capable of providing a law enforcement agency with information to which it may be entitled under statutes relating to electronic surveillance. Notably, section 1002(a)(2) provides, in pertinent part, as follows:

(a) Capability requirements . . . [A] telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of –

. . .

- (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 –
- (A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and
- (B) in a manner that allows it to be associated with the communication to which it pertains,

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)[.]

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

The first question to be resolved is whether cell site information constitutes "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). If so, then the Pen/Trap Statute allows for such information to be recorded or decoded by a pen register or trap and trace device, so long as the applicant for the § 3123 order certifies "that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that [law enforcement] agency." 18 U.S.C. § 3122(b)(2).

In *SDNY*, the court concluded that cell site information was indeed "signaling information."

In reaching that conclusion the court stated,

The term "signaling information" was added by the USA PATRIOT Act in 2001. See Pub. L. No. 107-56, § 216(c)(2), 115 Stat. 272, 290 (2001). Prior to the enactment of the USA PATRIOT [A]ct, the District of Columbia Circuit had held in connection with its interpretation of a related statute, 47 U.S.C. § 1001(2), that because a cell phone sends "signals" to cellphone towers in order to operate, the term "signaling information" includes information on the location of cell site towers used by a cellular telephone. See United States Telecom. Ass'n v. FCC, 227 F.3d 450, 458, 463-64 (D.C. Cir. 2000). While one cell site decision notes an absence of legislative history indicating that Congress intended cell site data to be included in this term when it enacted the USA PATRIOT Act, see Texas Decision, 396 F. Supp. 2d at 761, the language enacted is not so limited. Indeed, the legislative history reflects that the language regarding "signaling information" would apply "across the board to all communications media." H. R. Rep. No. 107-236(I), 107th Cong., 1st Sess., available at 2001 WL 1205861, at *53 (Oct. 11, 2001). Accordingly, we will interpret this provision in accordance with its most obvious meaning and the one that naturally would have been available to Congress, through the United States Telecom case, when the statutory language was enacted in 2001. See Lorillard v. Pons, 434 U.S. 575, 581 (1978) ("Where... 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.").

SDNY, at *3. Having independently reviewed the above-referenced sections of the House Report on the PATRIOT Act as well as the D.C. Circuit's decision in *United States Telecom.*, I find the reasoning in SDNY to be persuasive and therefore agree that cell site data, i.e., information on the location of cell site towers used by a cellular telephone, is included in the term "signaling information" for purposes of the Pen/Trap Statute. Such being the case, cell site information would be obtainable via the Pen/Trap Statute, unless obtaining such information pursuant to that statute was otherwise prohibited. This then takes me back to 47 U.S.C. § 1001, et seq.

Title 47 U.S.C. § 1001(2) defines the term "call-identifying information" as follows:

The term "call-identifying information" means 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.

47 U.S.C. § 1001(2).

However, and to reiterate, section 1002(a)(2) provides that

with regard to information acquired <u>solely</u> pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), . . . call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)[.]

47 U.S.C. § 1002(a)(2) (emphasis added). Thus, cell site/signaling information cannot be obtained "solely" pursuant to the authority of the Pen/Trap Statute if the disclosure of such cell site/signaling information "may disclose the physical location of the subscriber." Because cell site information indeed "may disclose the physical location of the subscriber," it follows that, pursuant to the provisions of 47 U.S.C. § 1002(a)(2), cell site information cannot be obtained *solely* pursuant to the Pen/Trap Statute. Reaching this conclusion then begs for an answer to the following question: if cell site information cannot be obtained solely pursuant to the Pen/Trap Statute, what authority (if any) in addition to, or instead of, the Pen/Trap Statute is needed in order for the government to obtain cell site information from a telecommunications carrier?

According to the government and according to the court in the *SDNY* case, that additional, or supplemental, authority is the SCA, specifically, section 2703(d), which allows for the issuance of a court order if "the governmental entity offers 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." By contrast, according to the courts in the *Southern Texas*, *EDNY*, and *Maryland* cases, that alternative and exclusive authority is Fed. R. Crim. P. 41, which allows for the issuance of an order compelling disclosure of information based on a finding of probable cause.

As the court in the *SDNY* case observed, the exception clause in section 1002 does not contain a direction that no cell site information may be obtained "pursuant" to the Pen/Trap Statute. Instead, it states that such information may be not be obtained "solely" pursuant to that statute.

The use of the word "solely" is significant. "Solely" means "without another" or "to the exclusion of all else." See Merriam-Webster's Collegiate Dictionary (10th ed. 2000), at 1114. If we are told that an act is not done "solely" pursuant to some authority, it can only mean that the act is done pursuant to that authority "with [] another" authority. Id. As a result, the use of the word "solely" in section 1002 necessarily implies that "another" mechanism may be combined - albeit in some unspecified way - with the Pen Register Statute to authorize disclosure of cell site information.

SDNY, at *6. The SDNY court then proceeded to consider, analyze and reject two propositions: (1) that cell site data can be obtained without any reliance on the Pen/Trap Statute and (2) that cell site data is not obtainable at all. See id. at *6-7. The court concluded that Congress intended cell site data to be captured by some means in addition to a pen/trap and trace device, and that means is found in the SCA, 18 U.S.C. § 2703. The court held as follows:

In sum, section 2703 is the most obvious candidate to be used in combination with the Pen Register Statute to authorize the ongoing collection of cell site information because it covers cell site information generally. Section 2703's absence of procedural provisions that typically attach to the transmission of ongoing information is explained by the fact that the pen register is the proper "device" to obtain cell-site information. Thus, the Pen Register Statute's procedural provisions that are tied to such a device are appropriately combined with an application under section 2703 to obtain such information.

Id. at *13. It is at this point that I respectfully depart company with my colleague in the Southern District of New York.

Because the exception found in 47 U.S.C. § 1002(a)(2) is central to the decision in this case, as it has been in all of the other court decisions dealing with the issue, it is appropriate to examine the legislative genesis of that provision. The legislative history of 47 U.S.C. § 1001, et seq. indicates

that, during his testimony before the Senate and House with respect to CALEA, then FBI Director Louis Freeh addressed, *inter alia*, what he thought was Congress's concern that legislation requiring telecommunications carriers to provide what the Director referred to as "call setup information" would permit the tracking of persons. During the course of his testimony, Director Freeh, while discussing the term "call setup information," stated the following:

The term "call setup information" is essentially the dialing information associated with any communication which identifies the origin and destination of a wire or electronic communication obtained through the use of a pen register or trap and trace device pursuant to court order. It does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called "tracking" information.

(Statement of Louis J. Freeh, Director, FBI, Before the Senate Judiciary Subcomm. on Tech. and the Law and the Subcomm. on Civil and Constitutional Rights, March 18, 1994, Federal Document Clearing House, at *23 available at 1994 WL 223962.)

Furthermore, in that portion of his testimony addressing the subject "Allegations of 'Tracking' Persons," Director Freeh attempted to allay Congress's concerns and stated as follows:

Law enforcement's requirements set forth in the proposed legislation include an ability to acquire "call setup information." This information relates to dialing type information -- information generated by a caller which identifies the origin, duration, and destination of a wire or electronic communication, the telephone number or similar communication address. Such information is critical to law enforcement and, historically, has been acquired through use of pen register or trap and trace devices pursuant to court order.

Several privacy-based spokespersons have criticized the wording of the definition regarding this long-standing requirement, alleging that the government is seeking a new, pervasive, automated "tracking" capability. Such allegations are completely wrong.

Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this 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, 468 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.

In order to make clear that the acquisition of such information is not being sought through the use of pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: except that such information (call setup information) shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange.

(Statement of Louis J. Freeh, at *29.)

Of course, the actual language that found its way into the statute was somewhat different than that proposed by Director Freeh. Instead of making clear that "call setup information" was not to include "any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange," the statute 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 (except to the extent that the location may be determined from the telephone number)[.]" 47 U.S.C. § 1002(a)(2). Nevertheless, what is abundantly clear from the foregoing excerpt of Director Freeh's testimony is that the language which found its way into the law was predicated on the Director's assertion to Congress that, in the government's view, pen register and trap and trace devices were not to be, and would not be, used to secure location information for the cellular phone user. Yet, it is precisely the Pen/Trap Statute upon which the government relies (at least in part) in seeking the instant order.

Most recently, in *In re Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information*, Misc. No. 05-508 (D.D.C. January 6, 2006) (the "*DC Case*" or "*DC*"), Magistrate Judge Facciola grappled with the same (or at least materially similar) issue with which the courts in *Southern Texas, EDNY, Maryland*, and *SDNY*, had grappled (and with which I am now grappling). After reviewing much of the same testimony of Director Freeh as quoted above, Judge Facciola stated,

[Whatever] the actual existence of the technology in 1994, I cannot find any contemporaneous understanding by either Director Freeh or the Congress that the government had the capability that it now has to ascertain the location of a person using a cell phone, let alone that Congress intended to permit the government to use the Pen Register statute to avail itself of that technology, provided it combined its use of that statute with some other means. While the government would counter, relying on Judge Gorenstein's opinion, that the word "solely" in 47 U.S.C. § 1002(a)(2) suggests that this is true because it only precludes use of the Pen Register statute itself, I would have to answer that this conclusion, besides being historically inaccurate, reaches an utterly counter-intuitive conclusion. It is inconceivable to me that the Congress that precluded the use of the Pen Register statute to secure in 1994 "transactional data" or what Freeh called "call [set]up information" nevertheless intended to permit the government to use that same statute, whether by itself or combined with some other means, to secure the infinitely more intrusive information about the location of a cell phone every minute of every day that the cell phone was on. I cannot predicate such a counter-intuitive conclusion on the single word "solely."

DC, at 11. I agree with Judge Facciola's comments. To be sure, that which the government is seeking in the instant application is not "information about the location of a cell phone every minute of every day that the cell phone was on." Id. Instead, the government is only seeking the location(s) of the cell towers being used by the cell phone at the commencement and termination of calls. But, even such less precise location information was included in the "tracking information" about which Congress was concerned and to which Director Freeh's mollifying remarks were directed. To reiterate, Director Freeh testified, inter alia, that "[s]ome cellular carriers do acquire information

relating to the general location of a cellular telephone for call distribution analysis purposes. However, this 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." Nevertheless, in an effort to assuage Congress's concerns, Director Freeh went on to state that

[i]n order to make clear that the acquisition of such information is not being sought through the use of pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: except that such information (call setup information) shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange.

(Statement of Louis J. Freeh, at *29.)

Moreover, there is yet a further reason why I find the government's "hybrid" authority argument to be unpersuasive. Again, during the course of his testimony before Congress, Director Freeh stated the following in response to a letter directed to him "falsely" alleging that the government was "seeking to 'dictate to industry' a new capability to acquire 'minute-by-minute surveillance of individuals' through transactional data":

This is a false issue for a number of reasons.

First, as is clearly set forth in the "purpose" section of the proposed legislation, the intent of the legislation is to maintain existing technical capabilities and to "clarify and define the responsibilities of common carriers . . . to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information under Chapters 119 and 206 of Title 18 and Chapter 36 of Title 50.11.["] These chapters have nothing to do with "transactional information" under our federal electronic surveillance and privacy laws. All telecommunications "transactional" information is already protected by federal law and is exclusively dealt with in Chapter 121 of Title 18 of the United States Code

("Stored Wire and Electronic Communications and Transactional Records Access")
The proposed legislation does not relate to Chapter 121 of Title 18.

(Statement of Louis J. Freeh, at *27-28) (emphasis added).

Simply stated, in his remarks, Director Freeh assured Congress that the legislation about which he was testifying and urging Congress to pass had nothing to do with, and did not relate to, the SCA, to wit, 18 U.S.C. § 2701, et seq. In the face of such testimony, it makes no sense to me that, by the use of the word "solely" in 47 U.S.C. §1002(a)(2), Congress was in some back-handed fashion intending to allow the SCA to be used in conjunction with the Pen/Trap Statute to obtain the very information that Director Freeh assured Congress he was not seeking the authority to obtain under the proposed legislation.

The bottom line is that the array of statutes invoked by the issues in this case, i.e., the Pen/Trap Statue, the SCA, and CALEA present much more a legislative collage than a legislative mosaic. If Congress intended to allow prospective cell site information to be obtained by means of the combined authority of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the statutes themselves. Indeed, for the reasons set forth above, the legislative history of CALEA would suggest Congress's intent to be otherwise.

Accordingly, and for all of the foregoing reasons, the government's application will be denied. That having been said, the issue presented by the instant application will undoubtedly raise its head again (at a minimum, when I am no longer on criminal duty and one of the other magistrate judges in this district is). I therefore encourage the government to expeditiously seek review of this order with the duty district judge.

NOW THEREFORE IT IS ORDERED that the government's application for an order authorizing the disclosure of prospective cell site information exclusively pursuant to the combined authority of 18 U.S.C. §§ 2703 and 3122 be and hereby is **DENIED**.

Your attention is directed to 28 U.S.C. § 636(b)(1)(A), Federal Rules of Criminal Procedure 59(a), and General Local Rule 72.3 (E.D. Wis.), whereby written objections to any order herein or part thereof may be filed within ten days of the date of service of this order. Failure to object in accordance with the rules cited herein waives your right to review.

SO ORDERED this 17

WILLIAM F CALLAHAN IP

United States Magistrate Judge

day of January 2006, at Milwaukee, Wisconsin.