



U.S. Department of Justice

Criminal Division

Office of Enforcement Operations

Washington, D.C. 20530

CRM-200800622F

JUN 1 2009

Ms. Catherine Crump
Staff Attorney
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, NY 10004

Dear Ms. Crump:

This is in response to your request of September 1, 2008, for access to records pertaining to the use of mobile phone records for law enforcement purposes.

We located (items 1- 7) in the Criminal Division within the scope of your request. We have processed your request under the Freedom of Information Act and will make all records available to you whose release is either required by that statute, or considered appropriate as a matter of discretion.

In light of our review, we have determined to release item 1 in full; items 2-5 in part and to withhold items 6-7, (as described on the enclosed schedule), in full. We are withholding the records and portions of records indicated pursuant to one or more of the following FOIA exemptions set forth in 5 U.S.C. 552(b):

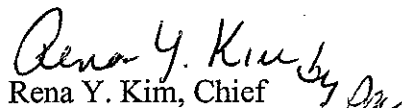
- (2) which permits the withholding of information relating solely to the internal personnel rules and practices of an agency;
- (5) which permits the withholding of inter-agency or intra-agency memorandums or letters which reflect the predecisional, deliberative processes of the Department;
- (7) which permits the withholding of records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information...
 - (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.

Please note that Items 3 and 5 are basically duplicates of documents that were referred to our Unit by the Executive Office for U.S. Attorneys (EOUSA). The only difference in the documents is the e-mail addresses listed at the top of some of the documents. We have determined, in our discretion, that these Items may be released with excisions. An exact set of the documents referred from the EOUSA is attached.

You have a right to an administrative appeal of this partial denial of your request. Your appeal should be addressed to: The Office of Information Policy, United States Department of Justice, 1425 New York Ave., NW, Suite 11050, Washington, DC 20530-0001. Both the envelope and the letter should be clearly marked with the legend "FOIA Appeal." Department regulations provide that such appeals must be received by the Office of Information Policy within sixty days of the date of this letter. 28 C.F.R. 16.9. If you exercise this right and your appeal is denied, you also have the right to seek judicial review of this action in the federal judicial district (1) in which you reside, (2) in which you have your principal place of business, (3) in which the records denied are located, or (4) for the District of Columbia. If you elect to file an appeal, please include, in your letter to the Office of Information Policy, the Criminal Division file number that appears above your name in this letter.

Sincerely,


Rena Y. Kim, Chief
Freedom of Information/Privacy Act Unit
Office of Enforcement Operations
Criminal Division

SCHEDULE OF DOCUMENTS WITHHELD IN FULL
(Refer to Body of Letter for Full Description of Each Exemption)

6. Email, 2/29/08, Mark Eckenwiler (Criminal Division), 1 page.

Withheld in full pursuant to 5 U.S.C. 552 (7)(E)

Withheld in part pursuant to 5 U.S.C. 552 (b)(2)

7. Email, 11/23/07, Mark Eckenwiler (Criminal Division), 3 pages.

Withheld in full pursuant to 5 U.S.C. 552 (b)(5) and (7)(E)

Withheld in part pursuant to 5 U.S.C. 552 (b)(2)

Inserts to Provider Order

IT IS FURTHER ORDERED that, pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, [CARRIER] and any other communication service providers, as defined in Section 2510(15) of Title 18, United States Code, during the authorized period of the interception over the TARGET PHONE, shall assist agents of the [AGENCY] by providing all information, facilities and technical assistance needed to ascertain the physical location of the TARGET PHONE, including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) TARGET PHONE (the "Requested Location Information"),² for a period of thirty (30) days.

IT IS FURTHER ORDERED that [CARRIER] shall disclose the Requested Location Information concerning the TARGET PHONE, and initiate a signal to determine the location of the TARGET PHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and shall furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, at any time of day or night, owing to the potential need to locate the TARGET PHONE outside of daytime hours.

IT IS FURTHER ORDERED that the furnishing of said information, facilities, and technical assistance by [CARRIER] shall terminate thirty days measured from the earlier of the day on which the investigative or law enforcement officers begin to conduct the interception of wire communications, pursuant to this Order or ten days from the date of the order is entered, unless otherwise ordered by this Court.

During the period of this Court's Order, the furnishing of such information, facilities and assistance by [CARRIER] and other communication service providers, shall be compensated for by the United States at the prevailing rate.

²Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call.

Inserts to Application

IT IS FURTHER REQUESTED, pursuant to Federal Rule of Criminal Procedure 41, that the Court issue an Order directing [CARRIER] to assist agents of the [AGENCY] by providing all information, facilities and technical assistance needed to ascertain the physical location of the TARGET PHONE, including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) the TARGET PHONE (the "Requested Location Information"),¹ for a period of thirty (30) days.

As explained in more detail in the Affidavit, there is probable cause to believe that the location of the TARGET PHONE at times determined by investigators will constitute or lead to evidence of the SUBJECT OFFENSES.

In light of the above, the government requests that this Court direct [CARRIER] to disclose the Requested Location Information concerning the TARGET PHONE, and to initiate a signal to determine the location of the TARGET PHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and to furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, at any time of day or night, owing to the potential need to locate the TARGET PHONE outside of daytime hours.

IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period of 30 days after the termination of the authorized period for acquisition of the Requested Location Information.

¹Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET PHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records – routinely retained by wireless carriers as business records – may only be obtained via a warrant issued on probable cause. See In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.).

Inserts to Order

IT IS FURTHER ORDERED that, pursuant to Rule 41(b) of the Federal Rules of Criminal Procedure, [CARRIER] and any other communication service providers, as defined in Section 2510(15) of Title 18, United States Code, during the authorized period of the interception over the TARGET PHONE, shall assist agents of the [AGENCY] by providing all information, facilities and technical assistance needed to ascertain the physical location of the TARGET PHONE, including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) TARGET PHONE (the "Requested Location Information"),³ for a period of thirty (30) days.

IT IS FURTHER ORDERED that [CARRIER] shall disclose the Requested Location Information concerning the TARGET PHONE, and initiate a signal to determine the location of the TARGET PHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and shall furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, at any time of day or night, owing to the potential need to locate the TARGET PHONE outside of daytime hours.

During the period of this Court's Order, the furnishing of such information, facilities and assistance by [CARRIER] and other communication service providers, shall be compensated for by the United States at the prevailing rate.

IT IS FURTHER ORDERED that the furnishing of said information, facilities, and technical assistance by [CARRIER] shall terminate thirty days measured from the earlier of the day on which the investigative or law enforcement officers begin to conduct the interception of wire communications, pursuant to this Order or ten days from the date of the order is entered, unless otherwise ordered by this Court.

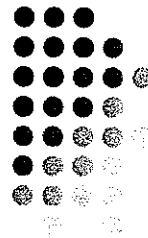
IT IS FURTHER ORDERED that the warrant for the Requested Location Information be returned to the issuing judicial officer within 10 days after the termination of the execution of the order.

IT IS FURTHER ORDERED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of notice may be delayed for a period of 30 days after the termination of the authorized period for acquisition of the Requested Location Information..

³Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call.

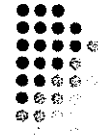
Current Legal Issues in Wireless Phone Location

Mark Eckenwiler
Associate Director
Office of Enforcement Operations



LAW ENFORCEMENT SENSITIVE
NOT FOR PUBLIC DISTRIBUTION

Overview



- Cellular technology
 - types of available location data
- Legal terrain
 - historical records
 - prospective location data
 - special constitutional and statutory issues

First Things First: A Common Vocabulary



- “Tower/sector” data
- “GPS” data
 - “lat-long” is more accurate
- Terms frequently misused or misunderstood
 - “cell site”
 - “ping”

3

Wireless Location Information and Provider Capabilities

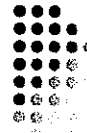


- Wireless networks necessarily require general information about user location
- CALEA (1994) requires carriers to be able to isolate and deliver certain user location data (tower and sector) to law enforcement at
 - origination of a call
 - answer of a call to the target phone
 - release (end of call) for both incoming and outgoing calls

4

Sample Data for Verizon Wireless Outbound Call

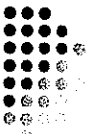
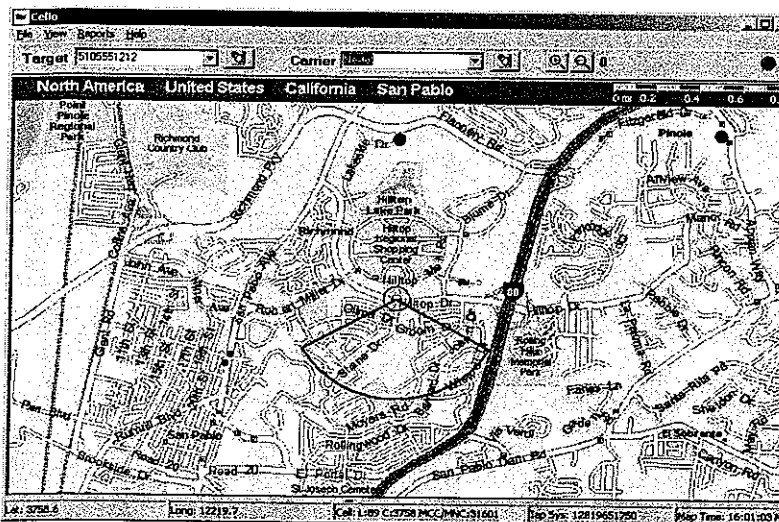
- Origination Message



5

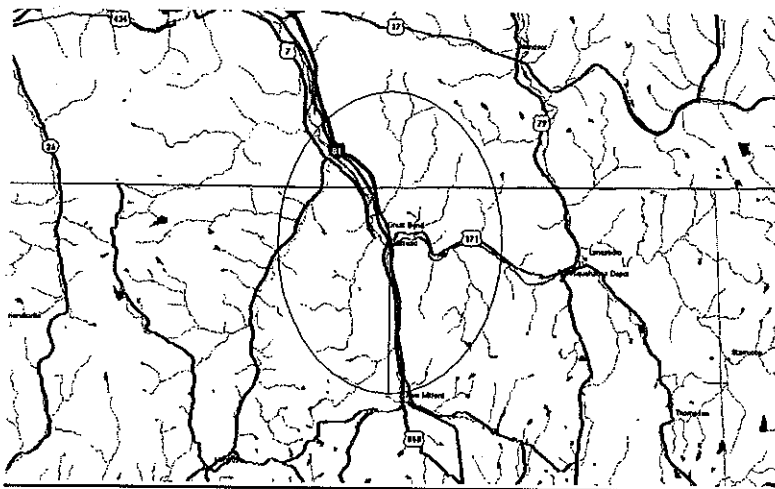
7e

Sample Tower/Sector



6

Omnidirectional Tower



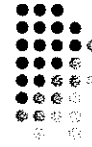
7

How Precise Is Tower/Sector Data?

- A cell tower's service radius can range from 200 meters to 30km
 - center city vs. suburbs vs. rural coverage
- Sector (tower face) information is not always provided with the tower identifier
- The tower closest to a phone does not necessarily serve every call to that phone
 - terrain
 - network load

8

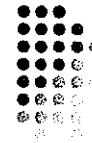
“GPS” Data (Latitude/Longitude)



- FCC “Enhanced 911” mandate requires wireless telephone carriers to be able to deliver certain location data for 911 calls
- Carriers may choose either of two ways to implement this capability
 - “handset solution”
 - “network solution”

9

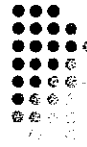
“Handset Solution” (True GPS)



- Phone itself contains a GPS device that calculates latitude/longitude
 - data resides on phone
 - carrier does not acquire location data absent 911 call (or active interrogation by carrier, where feasible)
- FCC requires accuracy:
 - to 50 meters for 67% of calls
 - to 150 meters for 95% of calls
- Used by Verizon, Sprint/Nextel*, Alltel

10

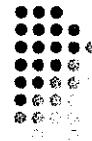
“Network Solution” (Signal Timing/Triangulation)



- Doesn't use GPS system *per se*
- Using any of various methods, measures signal characteristics relative to one or more towers
- FCC requires accuracy:
 - to 100 meters for 67% of calls
 - to 300 meters for 95% of calls
- Used by T-Mobile* and AT&T Wireless* (f/k/a Cingular)

11

Practical Limits






- Obviously, neither method works if phone is powered down

- carrier staff usually have to push a button each and every time lat/long data desired
- carriers typically impose a per-query or per-day charge

12

7E

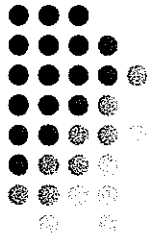
Practical Limits



7e

13

Legal Issues In Obtaining Location Data



14

Legal Roadmap



- Access to historical location data
- Access to prospective/ongoing location data
 - tower/sector
 - lat-long
 - assorted questions arising under Rule 41 & related statutes

15

Legal Authority for Acquiring Tower/Sector Data



- Historical tower/sector records: use court order under 18 USC 2703(d)
 - not an area of significant dispute
 - one outlier MJ opinion in W.D.Pa.; currently on appeal
- Prospective tower/sector records: use 2703(d) in combination with pen/trap (“hybrid theory”)
- CALEA (47 USC § 1002(a)(2)) restriction
 - “information that may disclose the physical location of the subscriber” **may not** be obtained from carrier “solely pursuant” to pen/trap authority
 - CALEA does not explicitly specify what additional authority suffices

16

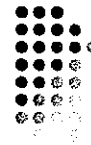
Judicial Decisions on Prospective Tower/Sector Data



- Magistrates in 12 districts have issued opinions rejecting the “hybrid” theory
 - variety of rationales
- Hybrid theory still accepted in numerous districts, including 3 where written opinions have issued
- To date, district court opinions are evenly split
 - unfavorable: N.D. Indiana, E.D. Wisconsin
 - favorable: S.D.N.Y., S.D. Texas

17

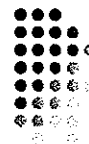
Decisions Rejecting “Hybrid” Theory



- Some judges rely on Fourth Amendment grounds
 - conflates lat-long data with less precise tower/sector data
 - inconsistent with *Miller* rule for business records
- Most simply find no express statutory mechanism available
 - § 2703(d) inapplicable (not prospective)
 - we must use Rule 41, by default

18

Access to Lat/Long Data



- Historical lat/long data typically does not exist
 - some exceptions exist, such as “kiddie-tracking” phones where logging is expressly part of service
- Prospective lat/long data: OEO recommends using Rule 41 search warrant
 - based on constitutional concerns, not statutory requirements
 - suggested forms (T-III insert and standalone) available; contact me for periodic updates

19

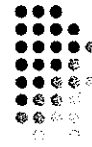
Summary of Legal Rules



	<i>Historical records</i>	<i>Prospective surveillance</i>
<i>Cell-site data (tower/sector)</i>	2703(d) order	“Hybrid” authority (2703(d) + pen/trap)
<i>Lat/long data (e.g., GPS)</i>	N/A (typically nonexistent)	Rule 41 warrant

20

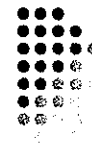
Issues in Applying Rule 41



- “Tracking device” provisions
- Timing: time of execution, duration
- Which district to apply to?
- Return
- Serving notice
 - timing & delay
 - persons to be given notice
- Standard for renewal

21

“Tracking Devices”: Rule 41 and 18 U.S.C. § 3117



- Rule 41 amended 12/1/06 to add procedures for use of “tracking devices”
- Cross-reference to § 3117 definition
 - “an electronic or mechanical device which permits the tracking of the movement of a person or object”
- Bottom-line advice: We believe that § 3117 – and thus the new Rule 41 provisions – **do not apply** because a user-operated cell phone is not a “tracking device”

22

“Tracking Device”: Why Does It Matter?



- Problematic interplay with Title III
 - “electronic communication” definition expressly excludes “any communication from a tracking device” (§ 2510(12)(C))
- § 3117 requires “installation”
 - 1986 legislative history focuses on types of physical devices at issue in *Knotts*, *Karo*
- Policy: avoid broad/literal reading
 - sweeps in ATMs, POS terminals, Internet devices!
- Several favorable opinions on point

23

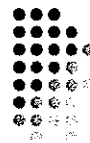
Rule 41 Warrants for Lat-Long Data: Where to Apply?



- Rule 41(b)(2)
 - warrant may issue for “a person or property outside the district if [it] is located within the district when the warrant is issued” but might subsequently move out of the district
- “Tracking device” provision (R. 41(b)(4))
 - “installation” must occur in district; outside use OK
- Conservative approach:
 - obtain warrant in district where phone is located
 - determine via tower data, visual surveillance, or CI
- Rely on § 2703(c)(1)(a) nationwide reach?

24

Rule 41 Warrants for Lat-Long: Time of Execution, Duration



- To avoid running afoul of daytime execution requirement, seek permission to execute outside of daytime hours
 - only need showing of "good cause"
- Duration
 - "Tracking device" provision allows 45 days
 - We recommend 30 days
 - better sync w/Title III, pen/trap cycles
 - obviates argument that duration is constitutionally excessive

25

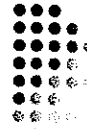
Rule 41 Warrants for Lat-Long: The Return



- Standard rule
 - "promptly return ... together with a copy of the inventory"
- "Tracking device" provision
 - must note "the exact date and time the device was installed and the period during which it was used"; return within 10 calendar days after use ends
- OEO advice: conform to tracking device rule
 - we would argue it's not necessary, but a reviewing court may disagree

26

Rule 41 Warrants for Lat-Long: Notice

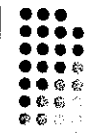


- Standard rule inapplicable
- Tracking device rule
 - within 10 calendar days after use ends, serve "person who was tracked or whose property was tracked"
- Issue: what if user isn't registered owner?
 - OEO advice: give notice to person tracked
-

27

re

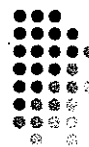
Rule 41 Warrants for Lat-Long: Renewal



- Tracking device provision permits renewal "for good cause"
- This is crazy
- Whether or not you rely on the tracking device provisions, make a fresh showing of probable cause
 - no different from a Title III extension in this respect

28

Summary



- Different types of wireless location data
 - Different legal analysis for tower/sector vs. more precise lat-long data
- OEO recommends invoking Rule 41 to obtain lat-long data
 - Anything less presents significant risks of suppression
 - Avoid Rule 41 "tracking device" provisions

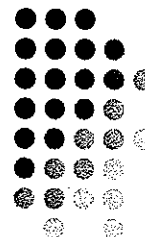
29

Questions?

Contact:
mark.eckenwiler@

[]

b2



30

Eckenwiler, Mark

From: Eckenwiler, Mark
Sent: Friday, September 12, 2008 2:38 PM
To: 'USAE0-CrimChiefs@usa.doj.gov'
Cc: [] b2
Subject: OEO guidance concerning requests for historical cellular telephone location information
Attachments: Final Memorandum of Law (WDPA).pdf; Exhibit C.PDF; reply -- final as filed.pdf

To: All USAO Criminal Chiefs
From: Office of Enforcement Operations, Criminal Division
Re: Guidance Concerning Requests for Historical Cellular Telephone Location Information
Date: September 12, 2008

A number of offices have inquired about a decision earlier this week from the District Court in W.D. Pa. that has received widespread press coverage. In the expectation that many of your local magistrate judges will be relying on this opinion, I am writing to offer guidance.

The case involves a request by the U.S. Attorney's Office in Pittsburgh for the wireless phone records of a suspected narcotics trafficker. The USAO sought to obtain cell-site records – that is, records showing the tower and tower face used at the start and end of calls – for a specified time period in the past, basing its request on 18 USC 2703(d) (requiring a showing of “specific and articulable facts,” a standard lower than probable cause).

Without requesting briefing on the law or the underlying technology, the magistrate judge (joined by four fellow magistrates) issued a lengthy opinion in February 2008 holding that such records may not be obtained absent a search warrant based upon probable cause. *See In re Application*, 534 F. Supp. 2d 585 (W.D. Pa. 2008). The USAO promptly appealed, only to have the district court summarily affirm in a two-page decision on Wednesday of this week.

As indicated in the attached opening brief and reply, we believe that both decisions are wrong on the facts as well as the law. Most importantly, the magistrate wrongly analyzed the request under the law governing prospective location surveillance, notwithstanding the fact that the USAO requested only historical records. In addition, the published opinion materially misstates the degree of precision of the requested records, conflating cell-site records – indicating the user's location at best only to within hundreds of yards – with more precise location information (such as GPS coordinates, typically unavailable for past periods). Both the magistrates and the district court ignored previous decisions in other districts explicitly endorsing the Department's position that historical tower/sector records may be compelled using a section 2703(d) order. *See In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007); *In re Application*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007). The USAO, in consultation with Criminal Division, is considering its options for seeking further judicial review.

Where agents seek to obtain GPS (or similarly precise) information for a target's phone on a prospective basis, OEO continues to recommend the use of a warrant under Rule 41. (Regularly updated model forms, either for standalone use or in connection with a Title III application, are available on request.)

9/29/2008

3

However, we remain firmly of the view that access to less-precise historical cell-site records, routinely kept by providers in the ordinary course of business, is governed by section 2703(d) and does not require a search warrant.

If you have any questions, or encounter difficulty on this issue with judges in your own district, please do not hesitate to contact me.

Mark Eckenwiler
Associate Director
Office of Enforcement Operations
Criminal Division

[62

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE)	
APPLICATION OF THE UNITED)	
STATES OF AMERICA FOR AN)	Magistrate's No.: 07-524
ORDER DIRECTING A PROVIDER)	
OF ELECTRONIC COMMUNICATION)	
SERVICE TO DISCLOSE RECORDS)	
TO THE GOVERNMENT)	

**GOVERNMENT'S MEMORANDUM OF LAW
IN SUPPORT OF REQUEST FOR REVIEW**

AND NOW comes the United States of America by its attorneys, Mary Beth Buchanan, United States Attorney for the Western District of Pennsylvania, and Soo C. Song, Assistant United States Attorney for said district, and hereby seeks review of the Opinion and Memorandum Order entered on February 19, 2008, by United States Magistrate Judge Lisa Pupo Lenihan at Magistrate's No. 07-524M, denying an application by the United States seeking disclosure of historical cell-site information pursuant to Sections 2703(c) & (d) of the Stored Communications Act ("SCA"), 18 U.S.C. § 2703(c) & (d) (the "Opinion and Order").¹ Copies of the Application and the Opinion and Order are attached as Exhibits A (filed separately under seal) and B, respectively. For the reasons set forth below, the government respectfully submits that this Court should reverse the Magistrate Judge's order and grant the Application in the instant case.

I. FACTUAL AND PROCEDURAL HISTORY

A. Historical Cell-Site Information

Cellular telephone companies keep, in the regular course of their business, records of certain

¹ The Opinion and Order has since been published as *In re Application of the United States*, 534 F. Supp. 2d 585 (W.D. Pa. 2008). Although authored by Magistrate Judge Lenihan, the Opinion and Order was signed by all but one of the Magistrate Judges in this district.

information associated with their customers' calls. Exhibit C contains an exemplar of these records from a major carrier, Sprint-Nextel, the same carrier whose records are at issue in the present case.² As reflected in Exhibit C, the records include for each call a customer made or received: (1) the date and time of the call; (2) the telephone numbers involved; (3) the cell tower to which the customer connected at the beginning of the call; (4) the cell tower to which the customer was connected at the end of the call; and (5) the duration of the call. The records may also, but do not always, specify a particular sector of a cell tower used to transmit a call.³ No such record is created when the phone is not in use.

Cell tower information is useful to law enforcement because of the limited information it provides about the location of a cell phone when a call is made. As one court has explained:

The information does not provide a "virtual map" of the user's location. The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas.

In re Application of United States for an Order for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (citation omitted). No Global Positioning System ("GPS"), that is, satellite-derived data, or other precision location information is contained in the historical records provided pursuant to the requested orders. Indeed, cell-site records do not even indicate a phone's distance from the serving tower, let alone its specific location.

² Because these records contain sensitive information pertaining to a recent investigation, certain identifying information – the telephone numbers involved – has been redacted.

³ Cell towers are often divided into three 120° sectors, with separate antennas for each of the three sectors. To the extent this information does exist in a particular instance, it does not provide precise information regarding the location of the cell phone at the time of the call, but instead shows only in which of the three 120°, pie-slice sectors the phone was probably located.

B. The United States' Application Pursuant to 18 U.S.C. § 2703(d) in this Investigation

Pursuant to 18 U.S.C. § 2703(c)(1), the United States may require a provider of electronic communication service to disclose "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)" when it obtains a court order for such disclosure pursuant to 18 U.S.C. § 2703(d) (hereinafter, a "2703(d) order"). A 2703(d) order is issued by a court when the government provides "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).

On February 22, 2008, the United States filed an application with Magistrate Judge Lenihan seeking a 2703(d) order directing Sprint Spectrum to disclose certain historical connection and cell-site information associated with a specified cell phone. *See Exhibit A.* The cell phone records are relevant and material to an ongoing investigation into large-scale narcotics trafficking and various related violent crimes.

In June 2007, the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF") learned from a confidential source that a particular subject and his associates use their wireless telephones to arrange meetings and transactions in furtherance of their drug trafficking activities. Additional investigation, along with information from the source, indicates that the subject's narcotics supplier lives in another state. Because the subject and his confederates use a variety of vehicles and properties to conduct their illegal activities, physical surveillance has proven difficult. In order to develop better information on the location and identity of the drug supplier, the instant Application seeks historical cell-site records concerning a phone known to be used by the subject. Section

2703(d) orders are broadly used and widely accepted for these types of purposes in federal criminal investigations across the country.

On February 19, the Magistrate Judge denied the Application, ruling in a written opinion that the United States is barred as a matter of law from obtaining historical cell-site information pursuant to a 2703(d) order.

II. ISSUE PRESENTED

The issue before the Court is purely a question of law, namely whether the government may obtain historical cell-site usage records pursuant to an order under 18 U.S.C. § 2703(d).

III. SUMMARY OF ARGUMENT

Section 2703(d) permits the government to obtain a court order compelling historical cell-site usage information from a wireless carrier. The plain language of the statute unambiguously states that the government may require “a provider of electronic communication service” to disclose “a record or other information pertaining to a subscriber” pursuant to a 2703(d) order. As explained below, historical cell-site information satisfies each element of the statute, a position endorsed in recent months by several other courts.

In reaching the opposite conclusion, the Opinion and Order contains numerous errors, both as to the facts of the underlying technology and as to the interpretation of applicable law. Indeed, as discussed below, we believe the Opinion and Order materially relies on at least one statute (and several cases) wholly inapplicable to the government’s request for stored records of past customer activity. In addition, because wireless carriers regularly generate and retain the records at issue, and because these records provide only a very general indication of a user’s whereabouts at certain times

in the past, the requested cell-site records do not implicate a Fourth Amendment privacy interest. Because the Opinion and Order misstates both the relevant facts and the applicable law, we respectfully urge the Court to reverse.

IV. ARGUMENT

A. Historical Cell-Site Information Falls Within the Scope of Sections 2703(c) and (d)

As the Third Circuit has often reiterated, “[t]he plain language of the statute is the starting place in our inquiry.” *United States v. Introcaso*, 506 F.3d 260, 264 (3d Cir. 2007) (quoting *Staples v. United States*, 511 U.S. 600, 605 (1994)). “If the language of a statute is clear[,] the text of the statute is the end of the matter.” *Id.* (quoting *United States v. Jones*, 471 F.3d 478, 480 (3d Cir. 2006)).

The Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.*, establishes a comprehensive framework regulating government access to customer records in the possession of communication service providers. The statute’s structure reflects a carefully crafted series of Congressional judgments; it distinguishes not only between communications contents (§ 2703(a), (b)) and non-content records (§ 2703(c)), but also between different classes of non-content records.

18 U.S.C. § 2703 unambiguously states that the government may require “a provider of electronic communication service” to disclose “a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)” pursuant to a 2703(d) order.⁴ See 18 U.S.C. § 2703(c)(1). As explained below, cell-site information quite

⁴ As noted above, a 2703(d) order is issued by a court when the government provides “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

clearly satisfies each of the three elements necessary to fall within the scope of this provision.

First, a cell phone company is a provider of electronic communication service. “Electronic communication service” is defined to mean “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. §§ 2510(15) & 2711(1). Cell phone service providers provide their customers with the ability to send wire communications, and thus they are providers of electronic communication service. *See* 18 U.S.C. § 2510(1) (defining wire communications).

Second, cell-site information constitutes “a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).” Historical cell-site information is a record stored by the provider concerning the particular cell tower used by a subscriber to make a particular cell phone call, and it is therefore “a record or other information pertaining to a subscriber or customer.” *See In re Application of United States for an Order for Disclosure of Telecommunications Records*, 405 F. Supp.2d 435, 444 (S.D.N.Y. 2005) (noting that cell-site data is “information” and “‘pertain[s]’ to a subscriber...or customer of cellular telephone service”).

Third, cell-site information is non-content information, as it does not provide the content of any phone conversation the user has over the cell phone. *See* 18 U.S.C. § 2510(8) (defining the “contents” of a communication to include information concerning its “substance, purport, or meaning”). Thus, because historical cell-site information satisfies each of the three elements of § 2703(c)(1), its disclosure may be compelled pursuant to 2703(d) order.

While the statute is unambiguous and thus resort to the legislative history is unnecessary, the

relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

legislative history of § 2703(c)(1) nevertheless confirms that it encompasses cell-site information. When the SCA was first enacted as part of the Electronic Communications Privacy Act (“ECPA”) in 1986, it permitted disclosure pursuant to a 2703(d) order (or subpoena) of the same catch-all category of “record[s] or other information pertaining to a subscriber or customer of such service (not including the contents of communications)” now codified at 18 U.S.C. § 2703(c)(1). *See* ECPA § 201, P.L. 99-508, 100 Stat. 1848, 1862 (1986). The accompanying 1986 Senate report emphasized the breadth of the “record or other information” category of information: “the information involved is information about the customer’s use of the service[,] not the content of the customer’s communications.” S. Rep. No. 541, 99th Cong., 2d Sess. 38 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3592 (1986). Moreover, cellular telephones were one of the new technologies of particular importance to Congress when it enacted ECPA, so there is no basis to exclude cellular telephone usage records from the scope of § 2703. *See* H.R. Rep. No. 647, 99th Cong., 2d Sess. 20-21 (1986).

Numerous recent decisions confirm the government’s view that 2703(d) orders may be used to obtain historical cell-site records. For instance, in September 2007, United States District Court Judge Stearns in Boston reversed a magistrate judge’s denial of a 2703(d) application for such records. *See In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007) (“*Stearns D. Mass. Opinion*”). After conducting a careful analysis of the SCA’s text, Judge Stearns held that “historical cell site information clearly satisfies” the statute’s definitional requirements, rejecting the magistrate’s analysis and granting the application. *Id.* at 80.

The following month, Judge Rosenthal in Houston confronted a similar situation: a magistrate judge had denied the government’s application for, *inter alia*, historical cell-site data

under the authority of § 2703(d). *See In re Application*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007). Here, too, the district court found the magistrate's objections on this question wholly without merit, reversing and holding that "the Government's request for historical cell-site information is within the statutory authorization." *Id.* at *5.

And most recently, on March 26, 2008, a federal magistrate judge in Atlanta issued an opinion rejecting a defendant's motion to suppress historical cell-site records acquired by means of a 2703(d) order. *See United States v. Suarez-Blanca*, No. 1:07-CR-0023-MHS/AJB (N.D. Ga. Mar. 26, 2008) (copy attached as Exhibit D). In his opinion endorsing the government's approach, the magistrate noted – and disagreed with – the Magistrate Judge's Opinion and Order in the present case. *Id.* at 32-33.

B. No Other Authority Limits the Compelled Disclosure of Historical Cell-Site Information Pursuant to a 2703(d) Order

The Opinion and Order errs at the outset by proposing to answer a legal question that is simply not relevant to this case. Instead of addressing the question at hand – whether the government may obtain historical cell-site records via a 2703(d) order – the decision below places a great deal of emphasis on determining the proper authority for obtaining such information prospectively. Prospective cell-site information is not at issue in this case. The decision never fully recovers from this initial wrong turn, and as a result conflates the legal principles actually relevant to the government's Application.

In the course of the analysis, the Magistrate Judge cites several authorities as purported limits on the government's ability to compel disclosure of historical cell-site information pursuant to 2703(d) orders. In particular, the Opinion and Order concludes that 47 U.S.C. § 1002(a)(2); the

mobile tracking device provision of 18 U.S.C. § 3117; the text of § 2703 itself; the Fourth Amendment; and the Wireless Communication and Public Safety Act of 1999 (“WCPSA”) all bar the government from compelling disclosure of cell-site information via 2703(d) orders.

However, as explained below, the cited Title 47 provision applies only to prospective evidence-gathering, and not to the instant Application for an order compelling historical records. Section 3117 is likewise inapplicable because a user’s own phone is not a “tracking device” within the narrow meaning of that statute. On the other hand, § 2703 not only applies, but on its face permits the government’s current Application. Finally, the customer records at issue are not protected by the Fourth Amendment. As a result, none of these authorities prohibits or even limits compelled production of historical cell-site information pursuant to a 2703(d) order, and the Opinion and Order below should therefore be reversed.

1. 47 U.S.C. § 1002 Does Not Apply to Requests for Historical Records, and Therefore Does Not Prohibit Compelled Production of Historical Cell-Site Information Pursuant to a 2703(d) Order

The Opinion and Order below devotes enormous space to discussion of the 1994 Communications Assistance for Law Enforcement Act (CALEA). In particular, the decision below places great weight on the fact that CALEA, at 47 U.S.C. § 1002(a)(2), states that

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) ... shall not include any information that may disclose the physical location of the subscriber.

(Emphasis supplied.) However, the present Application neither invokes nor in any way relies on the pen register/trap and trace statute. On the contrary, the government’s request – for historical, not future, cell-site records – relies on the entirely separate authority of 18 U.S.C. § 2703(d).

Because the CALEA provision quoted above mentions only the pen/trap statute, and not

§ 2703(d), it would be wholly improper to read into it what Congress chose to omit. Under the longstanding canon of *expressio unius est exclusio alterius* (“the expression of one is the exclusion of the other”), a court should presume that if “Congress wanted to include such a requirement ... it knew exactly how to do so.” *United States v. Thornton*, 306 F.3d 1355, 1359 (3d Cir. 2002). In the case of CALEA, this omission can hardly be called accidental. Congress was well aware of § 2703(d) in its deliberations over CALEA; in fact, a separate portion of the Act amended § 2703(d) to raise the showing required of the government. *See* Pub. L. 103-414, § 207(a) (1994).⁵

The decision below simply disregards the fact that 47 U.S.C. § 1002 imposes limits only on the pen/trap statute, and not on § 2703(d). Instead, it leans heavily in its analysis on numerous cases applying the CALEA restriction to government requests for prospective collection of future cell-site records.⁶

⁵ Nor does *expressio unius* produce an absurd result in this instance. A pen register order may issue where the government has made a mere certification of relevance. *See* 18 U.S.C. § 3123(a)(1). In contrast, § 2703(d) imposes the higher “specific and articulable facts” criterion. *See* H. Rep. No. 827, 103d Cong., 2d Sess. 31 (1994) (noting that change in required 2703(d) showing from relevance to specific and articulable facts “rais[es] the standard”), *reprinted in* 1994 U.S. Code Cong. & Admin. News 3489, 3511.

⁶ Magistrates and district courts have disagreed over whether § 2703 and the pen register statute can be used together to compel disclosure of cell-site information prospectively, an issue not raised in this case. *Compare In re Application of United States for an Order for Prospective Cell Site Location Information*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (upholding “hybrid” use of 2703(d) orders and pen/trap statute to compel prospective disclosure of cell-site information) with *In re Application of United States for an Order Authorizing Use of a Pen Register and Trap and Trace Device*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (rejecting such hybrid orders).

However, as the Magistrate Judge's Opinion and Order concedes, *see* 534 F. Supp. 2d at 600, even judges who have rejected prospective hybrid orders for cell-site information have agreed that compelled disclosure of historical cell-site information pursuant to 2703(d) orders is proper. *See, e.g.,* 396 F. Supp. 2d at 327 (“The applicable statutes allow the government to obtain historical cell site information on the basis of a showing less exacting than probable cause, but do not allow it to obtain such information prospectively on a real-time basis.”).

The Magistrate's opinion acknowledges the prior decisions holding (or implying) that historical cell-site records may be obtained by way of § 2703(d). In the same breath, however, the decision below dismisses that same precedent with the surprising claim that the legal distinction between prospective and historical cell-site records is "largely-unexplained." 534 F. Supp. 2d at 603. In fact, the government submits that the distinction is indeed clear, depending as it does on the explicit wording and structure of the pertinent statutes.

In crafting the federal statutes regulating governmental access to telecommunications records, Congress has unambiguously distinguished between historical (stored) and future records. Most prominently, Chapter 121 of Title 18 (the Stored Communications Act, §§ 2701 *et seq.*) stands in contrast to the Wiretap Act (Chapter 119) and the pen register statute (Chapter 206), both of which exclusively regulate prospective, ongoing surveillance (of content and non-content, respectively). Thus, the mechanism for obtaining historical telephone calling records – a subpoena, as provided for at § 2703(c)(2)(C) – differs from the authority under the pen/trap statute for monitoring the telephone numbers of future calls to or from a target telephone.

The decision below improperly disregards this key aspect of the statutes. Because it wrongly relies on the CALEA limitation (and cases applying it) to conclude that the statutes "do not distinguish between historic[al] and prospective [cell-site records]," 534 F. Supp. 2d at 586 n.4, its analysis should be rejected.

2. The Statutory Provisions Concerning "Tracking Devices" Do Not Limit Compelled Disclosure of Historical Cell-Site Information

The Opinion and Order also asserts that the United States may not use a 2703(d) order here because historical cell-site information is a communication from a "tracking device" as defined in

18 U.S.C. § 3117. *See* 534 F. Supp. 2d at 601-07. The analysis, however, is simply not supportable. As explained below, “tracking device” communications are excluded only from the definition of “electronic communication”; cellular telephone calls are instead “wire communications,” a defined term with no comparable exclusion. Second, a user’s own wireless phone is not a “tracking device” within the narrow meaning of the statute.

The decision below relies heavily on 18 U.S.C. § 2510(12)(C), which excludes “any communication from a tracking device” from the definition of “electronic communication.” Under the reasoning of the Opinion and Order, this provision excludes cell-site records from the reach of ECPA. In reaching this conclusion, however, the opinion overlooks one crucial, plainly expressed statutory distinction: cellular telephone calls are not “electronic communications” under any circumstances. On the contrary, conventional cellular calls are instead “wire communications” as defined at section 2510(1).⁷ Of equal importance, the “wire” and “electronic” categories are mutually exclusive: a “wire communication” cannot, under the express terms of the statute, also be an “electronic communication.” *See* § 2510(12)(A) (“‘electronic communication’ ... does not include—(A) any wire or oral communication”). Thus, properly analyzed under the statute, historical cell-site information concerning a wireless telephone call is plainly “a record or other information pertaining to a subscriber” using a service provider’s network to send and receive “wire communications.” *See Stearns D. Mass. Opinion*, 509 F. Supp. 2d at 80 (reversing magistrate

⁷ The essential distinction is that a “wire communication” necessarily involves the human voice. *See* § 2510(1) (defining “wire communication”) and § 2510 (defining “aural transfer”); S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3565 (“cellular communications – whether they are between two cellular telephones or between a cellular telephone and a ‘land line’ telephone – are included in the definition of ‘wire communications’ and are covered by the statute”).

judge's contrary conclusion).

The decision below overlooks these clearly articulated distinctions. Instead, the opinion dwells at length on the definition of an inapposite term ("electronic communication"). Having done so, the Opinion and Order further distorts the statute by construing the clear phrase "record or other information pertaining to a subscriber" to exclude

information that is regarding or derived under a service (e.g., a tracking capability/function) that may be used to facilitate the provision of an electronic communication service (e.g., the transmission of voice/text material), but that is not *itself* an electronic communication service (as, e.g., by definition).

534 F. Supp. at 604 (footnote omitted). Because this unduly complicated interpretation – unsupported by even a single citation to the legislative history of the statute – does violence to the plain meaning of "pertaining to," this Court must reject it. *See Malloy v. Eichler*, 860 F.2d 1179, 1183 (3d Cir. 1988) ("Where the language of the statute is clear, only 'the most extraordinary showing of contrary intentions' justify altering the plain meaning of a statute.") (*quoting Garcia v. United States*, 469 U.S. 70, 75 (1984)).

In addition, the decision below errs in finding that the target cell phone was a "tracking device" within the meaning of 18 U.S.C. § 3117. This overly expansive reading runs contrary to the language, structure, and legislative history of ECPA, and it would significantly undermine privacy protections for users of communication networks.

The structure of 18 U.S.C. § 3117 makes clear that a "tracking device" is a homing device installed by the government. Specifically, 18 U.S.C. § 3117(a) applies only when a court is authorized to issue an order "for the installation of a mobile tracking device." It then provides that "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.” *Id.* Thus, the purpose of the tracking device statute is to provide a court with extra-territorial jurisdiction over use of tracking devices installed within its jurisdiction. Given the limited purpose of the tracking device statute, there is no basis for interpreting “tracking device” broadly to encompass devices which the government would never have any reason to apply to a court to install or use. *See Stearns D. Mass. Opinion*, 509 F. Supp. 2d at 81 n.11 (§ 3117 “governs the ‘installation’ of tracking devices. The ‘tracking’ of a cell phone does not require the installation of any sort of device.”); *In re Application*, 405 F. Supp. 2d 435, 449 n.8 (S.D.N.Y. 2005) (same).

The legislative history of § 3117 is equally clear that “tracking devices” are homing devices, not cell phones or other communications technologies. Most obviously, the 1986 House Report on ECPA cites the two landmark Supreme Court decisions concerning “beeper” homing devices, *United States v. Knotts*, 460 U.S. 276 (1983) (beeper installed in can of chloroform and used to track movements of car) and *United States v. Karo*, 468 U.S. 705 (1984) (beeper installed in can of ether expected to be used in production of cocaine). No mention is made of cellular telephones.

Likewise, 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 follows:

These are 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 whereabouts 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. 10 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin.

News 3555, 3564 (1986).

Even more revealing is the fact that the very same 1986 legislation⁸ addresses cellular telephone technology extensively in numerous other provisions unrelated to “tracking devices.” Congress enacted ECPA because the Wiretap Act “had not kept pace with the development of communications and computer technology.” S. Rep. No. 541, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3556 (1986). Cellular phones were one of the new technologies of particular importance to Congress, *see id.* at 2 & 9, and cellular technology is central to much of ECPA’s legislative history. *See id.* at 2, 4, 6-9, 11-12, 21, & 29-30.

Congress made clear that cellular communications were to be protected as wire communications by the Wiretap Act and the SCA. In particular, Congress amended the definition of “wire communication” to ensure that it encompassed cellular communications by inserting the phrase “including the use of such connection in a switching station” into 18 U.S.C. § 2510(1). *See* ECPA § 101, Pub. L. No. 99-508, 100 Stat. 1848 (1986). As noted by the Senate Report on ECPA, “[t]his subparagraph makes clear that cellular communications--whether they are between two cellular telephones or between a cellular telephone and a ‘land line’ telephone--are included in the definition of ‘wire communications’ and are covered by the statute.” S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), *reprinted in* 1986 U.S. Code Cong. & Admin. News 3555, 3565 (1986).

Despite this extensive discussion of cell phones throughout ECPA’s legislative history, there is not a scintilla of evidence in the legislative history that Congress intended cell phones to be classified as tracking devices. Instead, all discussion of tracking devices suggests that Congress

⁸ The tracking device statute was enacted as part of ECPA. *See* Pub. L. No. 99-508, 100 Stat. 1848, § 108 (1986).

understood tracking devices to be homing devices installed by the government.

There is no reason to supply "tracking device" with a meaning much broader than that intended by Congress, especially because doing so would deny many communications the privacy protection Congress intended them to have. If cell phones were classified as "tracking devices," text messages or e-mail transmitted from them would not be "electronic communications" under 18 U.S.C. § 2510(12)(C). As a result, such communications would fall outside the scope of the Wiretap Act, and it would no longer be a federal crime for an eavesdropper to intercept them. *See* 18 U.S.C. § 2511(1)(a) (criminalizing interception of wire, oral, and electronic communications). This result is plainly contrary to Congress's purposes in passing ECPA, and the Opinion and Order's expansive interpretation of "tracking device" should therefore be rejected.

Moreover, if "tracking device" were given the broad interpretation adopted below, nearly all communications devices would be tracking devices. Certainly any device relying on the cellular communication system (including many pagers, text messaging devices such as Blackberries, and cellular Internet systems) would be a "tracking device." The same is also true of banking ATMs, retail credit-card terminals, or even landline telephones (since it is possible to determine information about a person's location from his use of each). But the Magistrate Judge's reasoning extends much further. It is generally possible to determine the physical location of a user connected to the Internet, and the whereabouts of fugitives and other suspects are frequently discovered based on their use of Internet-connected computers. Treating all such devices as "tracking devices" grossly distorts § 3117's scope and purpose, and this Court should reject the Magistrate Judge's overly broad reading of the statute. *See United States v. Schneider*, 14 F.3d 876, 880 (3d Cir. 1994) (a court has an obligation to construe statutes to avoid absurd results).

A recent opinion from the Eastern District of California underscores all of these points:

No use of cell phones and cell towers for tracking was expressly contemplated, and perhaps was not even possible in 1986. Certainly the legislative history gives no such indication.

In addition, it would prove far too much to find that Congress contemplated legislating about cell phones as tracking devices. For example, if an agent presently used a cell phone to communicate the whereabouts of a suspect by using the phone's video feature while he was surveilling the suspect, one could fit this situation into the words of the statute—one was using an electronic device which “permitted” the tracking of the suspect. Or, take the example of the ubiquitous monitoring cameras, such as the “red light,” parking lot or freeway cameras. These cameras track the location of many persons, albeit in a confined location, and could also fit in with the words of the statute. It is best to take the cue from Congress in this respect of electronic tracking devices, and confine § 3117(b) to the transponder type devices placed upon the object or person to be tracked.

In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007).

Thus, even if it were the case that cellular telephone calls were “electronic communications” — as set forth above, they unquestionably are not — the “tracking device” exclusion from the definition of that term is irrelevant because a user’s own phone falls outside the narrow scope of that defined term.⁹ For this reason as well, the decision below should be reversed.

⁹ The Opinion and Order asserts that the use of tracking devices pursuant to 18 U.S.C. § 3117 requires probable cause. 534 F. Supp. 2d at 595. Even if a subscriber’s own cell phone were a “tracking device,” it would not follow that a Rule 41 warrant founded on a showing of probable cause would be required to obtain historical cell-site records. First, as the Advisory Committee Notes to the 2006 amendments to Rule 41 explain, if “officers intend to install and use the [tracking] device without implicating any Fourth Amendment rights, there is no need to obtain the warrant.” Fed. R. Crim. P. 41, Advisory Comm. Notes to 2006 Amendments, Subdivision (b). The Committee Notes further explain that “[t]he tracking device statute, 18 U.S.C. § 3117, does not specify the standard an applicant must meet to install a tracking device.” *Id.* at subdivision (d).

Indeed, the statute does not even prohibit the use of a tracking device in the absence of conformity with § 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

3. Section 2703(d) Does Not Permit a Court to Demand a Showing of Probable Cause

The Opinion and Order also asserts that § 2703 permits a court to demand a showing of probable cause as a precondition to issuance of a 2703(d) order. This conclusion allegedly flows from the express language and structure of § 2703. Instead, the text of the statute points to the opposite reading.

As before, “every exercise of statutory interpretation begins with an examination of the plain language of the statute.” *Rosenberg v. XM Ventures*, 274 F.3d 137, 141 (3d Cir. 2001). Where statutory language is “plain and unambiguous,” no further inquiry is necessary. *Id.* On its face, § 2703(d) demands a showing of “specific and articulable facts.” Nowhere does that subsection state, or even imply, that probable cause is or may be demanded.

Section 2703(c) permits the government to use any of various methods to obtain stored, non-content customer records. As the House Judiciary Committee noted in its report accompanying ECPA in 1986,

the government must use one of three sets of authorized procedures. The government can rely on administrative subpoenas or grand jury subpoenas to the extent that such processes are legally authorized. Alternatively, the government can use a search warrant. Finally, the government can seek a court order directing the disclosure of such records. If a court order is sought then the government must meet the procedural requirements of subsection (d).

H. Rep. No. 647, 99th Cong, 2d Sess. 69 (1986) (emphasis added). Current § 2703(c)(1) preserves this structure, explicitly making 2703(d) orders a means of compelling records separate from and alternative to a warrant based on probable cause. *Compare* § 2703(c)(1)(A) (authorizing use of search warrant under Rule 41) *with* § 2703(c)(1)(B) (authorizing use of 2703(d) court order).

section.”) (emphasis in original); *In re Application*, 405 F. Supp. 2d at 449 n.8 (same).

To do as the Magistrate Judge did below, and insist that a § 2703(d) application set forth probable cause, is in effect to demand a warrant, and thus to render part of the statute superfluous. This contravenes the longstanding canon that a court should, whenever possible, give effect to every provision of a statute. *See, e.g., Tavaréz v. Klingensmith*, 372 F.3d 188, 190 (3d Cir. 2004).

Even if the text of the statute were not clear on its face, an examination of the legislative history confirms Congress's intent that a 2703(d) court order be granted on less than probable cause. As originally enacted in 1986, § 2703(d) required only a showing that "there is reason to believe ... the records or other information sought, are relevant to a legitimate law enforcement inquiry." Pub. L. 99-508, § 201 (1986). Eight years later, Congress affirmatively chose to raise the test to the current "specific and articulable facts" standard. *See* Pub. L. 103-414, § 207(a) (1994). As the accompanying House Judiciary Committee report makes clear, this is "an intermediate standard ... higher than a subpoena, but not a probable cause warrant." H. Rep. No. 827, 103d Cong., 2d Sess. 31 (1994) (emphasis added), *reprinted in* 1994 U.S. Code Cong. & Admin. News 3489, 3511.

4. The Fourth Amendment Does Not Bar Compelled Disclosure of Historical Cell-Site Information Pursuant to a 2703(d) Order

Finally, the Opinion and Order suggests that a user has a reasonable expectation of privacy in historical cell-site information. 534 F. Supp. 2d at 610-11. This conclusion is incorrect for two distinct reasons. First, under the established principles of *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), there is no reasonable expectation of privacy in such information, and, accordingly, no Fourth Amendment-protected privacy interest. Second, historical cell-site information is far too imprecise by any measure to intrude upon a reasonable expectation of privacy. Thus, the Fourth Amendment does not limit disclosure of historical cell-site

information pursuant to 2703(d) orders.

The cell-site data that the government is seeking is not in the hands of the cell phone user at all, but rather is in the business records of a third party – the cell phone company. The Supreme Court has held that a customer has no privacy interest in business records of this kind. Addressing a Fourth Amendment challenge to a third party subpoena for bank records, the Court held in *United States v. Miller*, 425 U.S. 435 (1976), that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440; *see also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party ... he cannot object if the third party conveys that information or records thereof to law enforcement authorities"). Thus, an individual has no Fourth Amendment-protected privacy interest in business records such as cell-site connection information, to the extent the records are kept, maintained and used by a cell phone company in the normal course of business. If anything, the privacy interest in cell-site information is even less than the privacy interest in a dialed phone number or bank records. The location of the cell phone tower handling a customer's call is generated internally by the phone company and is not typically known by the customer. A customer's Fourth Amendment rights are not violated when the phone company reveals to the government its own records that were never in the possession of the customer.

The Court's reasoning in *Smith v. Maryland* leads to the same result. In *Smith*, the 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 applies equally to cell-site information. First, the

Court stated: “we doubt that people in general entertain any 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.” *Id.* at 742. Similarly, cell phone users understand that they must send a radio signal which is received by a cell phone company’s antenna in order to route their call to its intended recipient. (Indeed, cell phone users are intimately familiar with the relationship between call quality and radio signal strength, as typically indicated by a series of bars on their phones’ displays.)

Second, 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.” *Id.* at 743 (internal quotation 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.” *Id.* 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.” *Id.* at 744. Here, a cell phone user transmits a signal to a cell tower for his call to be connected and thereby assumes the risk that the cell phone provider will reveal the cell-site information to law enforcement. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no expectation of privacy in cell-site information.

As a business record in the possession of a third party, cell-site information should not be judged under Fourth Amendment standards for transponders and similar tracking devices surreptitiously installed by the government. However, even measured against the constitutional

standards articulated by the Supreme Court in this area, there is no reasonable expectation of privacy in cell-site information. The mere use of a tracking device, even when surreptitiously placed by the government, does not implicate Fourth Amendment privacy concerns. *See United States v. Knotts*, 460 U.S. 276, 282 (1983) (police monitoring of beeper signals along public roads did not invade any legitimate expectation of privacy). To be of constitutional concern, a surreptitiously installed tracking device must reveal facts about the interior of a constitutionally protected space. *See United States v. Karo*, 468 U.S. 705, 713 (1984) (distinguishing *Knotts* and holding that police monitoring of a beeper that disclosed information about the interior of a private residence, not open to visual surveillance, required a warrant).

The Opinion and Order's "Technological Development Overview" makes certain claims about wireless telephone location information: 1) that wireless phone companies "store cell tower registration histories" reflecting a phone's location at seven-second intervals; 2) that "the location of just the nearest tower itself can place the phone within approximately 200 feet"; and 3) that triangulation techniques or GPS capabilities make a user's location "precisely determinable" to within as little as 50 feet. 534 F. Supp. 2d at 589-90. The first two claims are demonstrably false, and the third claim (also incorrect) is irrelevant to the separate type of records sought in the instant Application.

On the first issue, the Opinion and Order is correct that a wireless phone, when first powered on, "registers" with a nearby tower, and that the phone thereafter periodically re-registers with the network over time. (Network awareness of a phone's approximate recent whereabouts makes delivery of incoming calls more efficient.) However, no "history" of these events is maintained: once a phone moves into the coverage area of a new tower and registers with it, the prior information

is no longer useful, and the network management software simply deletes the prior registration data. Put differently, the only “registration” data in a carrier’s possession at any given moment is the current information. No tower registration history is kept.

As Exhibit C makes clear, historical cell-site data retained by the carriers – that is, the category of information called for by the government’s Application in this case – reflects only the identity of the serving tower (and sector, if applicable) when the phone is in active use. The carrier recorded and preserved the cell-site information only at the start and end of actual telephone calls occurring over a few days. Plainly, a typical record such as Exhibit C does not even reveal the location of a nearby cell tower – let alone the phone user’s own location – at 7-second intervals.

In making the second claim, the Opinion and Order cites only to a single law student note, which says

[a] very general sense of a phone's is [sic] can be gathered by tracking the location of the tower being used during a call. In urban areas, where there are many towers, this may give a picture location [sic] within a couple hundred feet. In rural areas, towers may be miles apart. A slightly more accurate location picture can be generated by tracking which 120 degree “face” of the tower is receiving a cell phone's signal.

Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 Hastings Comm. & Ent. L.J. 421, 426-27 (Spring 2007). The author’s sole source for these claims is a recent decision, *In re Application of United States for an Order for Disclosure of Telecommunications Records*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005), which in fact contradicts the key assertion about precision in urban settings:

In suburban or rural areas, towers can be many miles apart. The Court has examined a map of cellular towers of a provider in lower Manhattan, which is one of the areas more densely populated by towers. In this area, the towers may be anywhere from several hundred feet to as many as 2000 feet or more apart.

[...]

The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas.

Id. at 437 & 449 (expressly rejecting claim that Fourth Amendment protects such general location information) (emphasis added).

The Opinion and Order's second claim also contradicts repeated findings of the Federal Communications Commission, which relies on the advice of skilled telecommunications engineers (both on FCC staff and those employed by carriers filing public comments). In one proceeding, for instance, the FCC found that a certain location-finding technique accurate to within 500-1000 meters (roughly 1640-3280 ft.) "would be significantly more precise" than "the location of the cell site or sector receiving the call." *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000).¹⁰ The Commission went on to note that simple cell-site information "can in some instances be misleading, as wireless calls are not always handled by the nearest cell." *Id.*

Given a stark choice between crediting a lone law student (in this case, one misstating the factual findings of a federal court) and the FCC, the government respectfully suggests to this Court that the FCC is more credible. For the same reasons, the Opinion and Order's claim that historical cell-site records "place the phone within approximately 200 feet" should also be rejected.

¹⁰ See also *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 16 FCC Rcd. 18305, 18311 n.49 (Oct. 12, 2001) (similar technique to locate phone within a 1000-meter radius held to be "a notable improvement in accuracy and reliability over ... the location of the cell site or sector receiving the call."); *In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 14 FCC Rcd. 17388, 17414 (Oct. 6, 1999) (accuracy of 285 meters – 311 feet – "would be far more accurate than ... cell site location information.") (emphasis added).

The Opinion and Order's third claim – that triangulation techniques or GPS capabilities currently make a user's location “precisely determinable” to within as little as 50 feet – is simply inapposite.¹¹ Those entirely distinct techniques relate to real-time (or prospective) location-finding capabilities, “Enhanced 9-1-1 Phase II” in FCC parlance. As noted explicitly in all of the FCC documents referenced above, these prospective location-finding capabilities have been imposed by the FCC for the very reason that cell-site data (“Phase I” information) is so imprecise.

Simply put, the government's present Application seeks only historical cell-site – that is, single-tower and sector – records. It does not seek GPS or “triangulation” information, which is in any event almost never available for past time periods.¹² Rather, the government has requested only the type of records shown in Exhibit C.

As an example, the first line of Exhibit C shows a May 1, 2007 call in the Boston area, Location Area Code 4361, from Cell ID 49874. A separate spreadsheet (supplied by the carrier) that contains only general information about tower attributes – that is, no information about specific customer activities or usage – reveals that Cell ID 49874 corresponds to face number 1 (of 3) on a

¹¹ As an aside, the government notes that this is also an exaggeration. Current FCC regulations for emergency (911) calls require that, by September 11, 2012 – more than four years hence – carriers be able to deliver location data at a level of 100 meters for 67 percent of calls and 300 meters for 95 percent of calls (for so-called “network-based” solutions), and 50 meters for 67 percent of calls and 150 meters for 95 percent of calls (for handset-based solutions). *See* 47 C.F.R. § 20.18(h)(1)(i), (ii). These requirements apply only to customer-initiated calls to a “public safety answering point” (911 operators). Moreover, the deadline for regulatory compliance has been delayed repeatedly in recent years, in large part because of carrier opposition or non-compliance.

¹² Carriers do not typically generate and retain more precise location records in the normal course. The exceptions to this general rule are so-called “kiddie tracker” phones, where – for a separate fee – some carriers offer a service for parents to monitor the movement of a child's phone. *See, e.g.,* <http://www.alltel.com/familyfinder>. These services are not included in standard feature packages, and are often restricted to certain handsets. *See, e.g., id.*

tower at a particular location north of Boston. Here, this means that the target phone was likely, but not necessarily, roughly northeast of the specified tower coordinates. It does not give the coordinates of the target phone itself, nor even an approximate indication of its distance from the tower; instead it only suggests an area tens of thousands (or more) square yards large in which the target phone was used. As noted above by the FCC, the fact that wireless calls are not always handled by the nearest cell further contributes to the generality and imprecision of this information.

Thus, cellular phone companies' historical records of cell-site usage are much too imprecise to tell whether calls have been made or received from a constitutionally protected space, let alone to reveal facts about the interiors of private homes or other protected spaces. *See* 405 F. Supp. 2d at 449 (cell-site information "does not provide a 'virtual map' of the user's location.... The information does not pinpoint a user's location within a building.").

As a final basis to support the notion that customers enjoy Fourth Amendment rights in the routine business records of their wireless providers, the Opinion and Order cites a range of statutes purportedly conferring constitutional rights. For instance, the decision below invokes the Wireless Communication and Public Safety Act of 1999 (WCPSA), 47 U.S.C. § 222(f), asserting that it "expressly recognizes the importance of an individual's expectation of privacy in her physical location." 534 F. Supp. 2d at 610.

In fact, however, the WCPSA offers no such recognition. Instead, the WCPSA simply 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 99-679, 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)). Thus, the WCSPA does not create or reinforce any constitutional expectation of privacy, and therefore imposes no bar to the disclosure of cell-site information pursuant to 2703(d) orders.

More importantly, a federal statute cannot in any event establish a constitutional norm. As the Fifth Circuit has observed in analyzing the Right to Financial Privacy Act,

[w]hile it is evident that Congress has expanded individuals’ right to privacy in bank records of their accounts, appellees are mistaken in their contention that the expansion is of constitutional dimensions. The rights created by Congress are statutory, not constitutional.

United States v. Kington, 801 F.2d 733, 737 (5th Cir. 1986) (emphasis supplied).

Thus, because there is no reasonable expectation of privacy in historical cell-site records, the Fourth Amendment does not limit compelled disclosure of such records pursuant to a 2703(d) order.

V. CONCLUSION

For these reasons, the government respectfully submits that this Court should reverse the Opinion and Order below and grant the Application in the instant case.

Respectfully submitted
MARY BETH BUCHANAN
United States Attorney

s/ Soo C. Song
SOO C. SONG
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 644-2645 (Fax)
soo.song@usdoj.gov
DC ID No. 457268

PAUL E. HULL
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 894-7311 (Fax)
paul.hull@usdoj.gov
PA ID No. 35302

MARK ECKENWILER
Associate Director
Office of Enforcement Operations
Criminal Division
U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530

NATHAN JUDISH
Senior Counsel
Computer Crime and Intellectual Property
Section
Criminal Division
U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530

8/7/2007 11:42 AM

Call Records for REDACTED CDR

1 of 54

Customer PTH	Date	Call Initiation Time	Duration (sec)	Type	Forwarded	911	International	Caller / Called PTR	Originating Call Site	Terminating Call Site
REDACTED	1-May-2007	12:07 PM	4	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	1-May-2007	12:28 PM	214	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	1-May-2007	5:57 PM	3	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	1-May-2007	5:57 PM	32	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	1-May-2007	5:59 PM	1202	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	1-May-2007	5:43 PM	88	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	2-May-2007	1:42 PM	288	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	2-May-2007	3:28 PM	93	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	2-May-2007	3:37 PM	722	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	2-May-2007	4:33 PM	47	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	2-May-2007	4:39 PM	8	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	2-May-2007	4:40 PM	23	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	2-May-2007	8:07 PM	6	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	2-May-2007	8:09 PM	125	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	2-May-2007	8:12 PM	85	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	2-May-2007	8:16 PM	65	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	3-May-2007	9:11 AM	62	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	3-May-2007	11:53 AM	14	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	3-May-2007	12:04 PM	497	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	3-May-2007	12:44 PM	601	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
REDACTED	3-May-2007	1:36 PM	281	Inbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874
	3-May-2007	1:40 PM	6	Outbound	No	No	No		NMA1708R_INIO2S3O_ (NENG-2) 4361 49874	NMA1708R_INIO2S3O_ (NENG-2) 4361 49874

REDACTED

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE)
APPLICATION OF THE UNITED)
STATES OF AMERICA FOR AN)
ORDER DIRECTING A PROVIDER)
OF ELECTRONIC COMMUNICATION)
SERVICE TO DISCLOSE RECORDS)
TO THE GOVERNMENT)

Magistrate's No.: 07-524

**GOVERNMENT'S REPLY MEMORANDUM OF LAW
IN SUPPORT OF REQUEST FOR REVIEW**

AND NOW comes the United States of America by its attorneys, Mary Beth Buchanan, United States Attorney for the Western District of Pennsylvania, and Paul E. Hull, Assistant United States Attorney for said district, and hereby files this reply to the memoranda of law filed by amici curiae Electronic Frontier Foundation et al. ("EFF"), Susan Freiwald, and the Federal Public Defender. For the reasons set forth below, the government respectfully asks this Court to reverse the Opinion and Order and grant the Application in the instant case.

SUMMARY OF ARGUMENT

At the outset, the Government commends amici EFF and Freiwald for acknowledging essential legal errors in the reasoning of the Opinion and Order below. For example, amici EFF and the Federal Public Defender admit that historical cell-site information is "a record or other information pertaining to a subscriber," and that it therefore falls within the scope of section 2703, contrary to the ruling below. *See* Brief of Amici Curiae Electronic Frontier Foundation et al. ("EFF Mem.") at 6-8; Brief of Amicus Curiae Federal Public Defender ("FPD Mem.") at 3 (amicus "does not agree that [cell-site location information] is excluded from protection under the [Stored Communications Act]").

Similarly, amicus EFF concedes that 47 U.S.C. § 1002 – upon which the Opinion and Order places so much weight – does not even apply to the Government’s present application for historical cell-site records. *See* EFF Mem. at 13. And both EFF and the Federal Public Defender acknowledge that the Opinion and Order mistakenly relies upon other, equally inapplicable federal statutes to support its erroneous conclusions. *See* EFF Mem. at 10-12 (discussing 18 U.S.C. § 3117, 47 U.S.C. § 222, and Rule 41); FPD Mem. at 2-3.

Notwithstanding these crucial concessions, amici put forward two main lines of argument in opposition to the Government’s appeal. First, amici claim that historical cell-site records are protected by the Fourth Amendment, and that governmental access to them requires a probable cause order. In addition, amici claim that law enforcement access to such records via a 2703(d) “specific and articulable facts” court order enables “dragnet surveillance,” and that a court has discretion to demand a showing of probable cause notwithstanding the express language of the statute. Neither set of claims survives examination, and the Court should therefore reverse the Opinion and Order below and grant the instant Application.

I. THE FOURTH AMENDMENT DOES NOT BAR COMPELLED DISCLOSURE OF HISTORICAL CELL-SITE RECORDS PURSUANT TO A 2703(d) ORDER

Amici argue at length that historical cell-site records enjoy Fourth Amendment protection. Specifically, they assert that such records “reveal[] an individual’s location in a private space.” EFF Mem. at 18; *see also* Freiwald Mem. at 2 (“CSLI, even if imprecise, will almost always indicate constitutionally-protected information about the inside of a home”). For several reasons, these contentions are wholly without merit.

A. Cell-Site Records Are Too Imprecise To Indicate
That A Wireless Phone Is Within a Constitutionally Protected Private Area

To begin with, amici provide no factual support whatsoever for their claims about the specificity of historical cell-site records. They neither rebut nor distinguish the authorities cited by the Government – including three separate FCC reports – establishing that cell-site records cannot identify a phone’s location more accurately than a range of a few hundred meters at best.¹ And amici simply ignore the sample records, attached to the Government’s opening brief as Exhibit C, illustrating that stored CSLI reveals only the location of the serving tower/face but not the precise location of the phone itself.²

Instead, amicus EFF attempts to diminish the importance of these sources – and, it would seem, to draw attention away from its own total failure to present factual information in support of its position – with the aside that “[t]he government quibbles with Magistrate Judge Lenihan’s factual findings.” EFF Mem. at 22. Even worse, amicus Freiwald speculates that “CSLI will grow only more precise over time,” Freiwald Mem. at 2, without offering any support for this claim. The Government respectfully submits that the Court should decide the pending Application on the basis of the facts before it, and not on amici’s vague speculation about distant future evolution of the relevant technology.

¹See Govt’s Mem. at 23-24 (quoting three FCC reports and one federal court opinion).

²Amicus Federal Public Defender sows confusion with its discussion (FPD Mem. at 10-11) of mid-call handoffs between cellular towers. Amicus does not establish that such handoffs – which occur as a routine matter literally millions of times a day across the U.S. – involve “triangulation” of the phone’s precise location. The Court need not resolve this factual question, however, for one simple reason: regardless of the Government’s request, no such purported “call handoff” location records are stored and retained by the carriers, as even a cursory examination of Exhibit C reveals.

B. Historical Cell-Site Records Are Created and Retained
 By Wireless Carriers in the Ordinary Course of Business,
 And Are Therefore Not Subject to a Reasonable Expectation of Privacy

In addition, amici offer contradictory assertions about the manner in which wireless carriers acquire and retain historical cell-site records. Amicus EFF correctly concedes that the records at issue in this proceeding are “routinely generated and recorded by the cell phone service provider in the ordinary course of providing communications service to its customer.” EFF Mem. at 6; *see also id.* at 30 (“CSLI is ... generated by the provider itself as part of its provision of service. ... The tower information is generated whenever the phone is on. The provider decides what historical tower call records to keep.”) In contrast, amicus Freiwald claims, without any support,³ that wireless carriers keep this information at the direction of law enforcement. *See* Freiwald Mem. at 13.

Given EFF’s concession, the Court can and should resolve any Fourth Amendment question under the rule articulated in *United States v. Miller*, 425 U.S. 435 (1976). Just as bank records “are not respondent’s ‘private papers’” but are “the business records of the banks” in which a customer “can assert neither ownership nor possession,” *id.* at 440, historical cell-site records are the business records – routinely created and retained without government compulsion – of wireless telephone carriers.

In that respect, historical cell-site records are no different from any other transaction records. For instance, records of past credit card transactions will often serve to place a person at a given location at a specific time, yet under established Fourth Amendment law they enjoy no Fourth Amendment protection. The novel contrary rationale urged by amici, taken to its logical conclusion,

³The sole basis for this claim is apparently the allegation in the Opinion and Order that carriers retain cell-site records “principally, if not exclusively, in response to Government directive.” Bare repetition of this unsupported claim does not make it a fact.

would require the Government to obtain a warrant before seeking such records (or bank ATM records, or even corporate records of employee time and attendance). The Court should decline the invitation to invent a previously unrecognized Fourth Amendment interest in this type of routinely gathered business record, and accordingly grant the Application.

C. Even If Analyzed Under the Supreme Court's Cases Concerning
"Tracking Devices," Government Access to Historical Cell-Site Records
Is Not A "Search" and Therefore Infringes No Fourth Amendment Interest

As noted in the Government's initial brief and above, cell-site information should be analyzed as a business record of a third party, and not under the Fourth Amendment doctrines relating to tracking devices. Even under the latter line of cases, however, government access to historical cell-site information does not infringe a constitutional privacy interest.

In arguing to the contrary, amici misstate the applicable Fourth Amendment doctrines. For instance, EFF insists that "*Knotts* and *Karo* stand for the proposition that there is a reasonable expectation of privacy in the presence of a person or object in a private place." EFF Mem. at 21; *see also* Freiwald Mem. at 8 (arguing that Fourth Amendment test under *Karo* is whether an object has been "withdrawn from public view"). As described below, amici have fundamentally misread *Karo*.

At issue in *United States v. Karo*, 468 U.S. 705 (1984), is not whether persons or objects in private spaces enjoy generalized and undifferentiated Fourth Amendment protection. Rather, as the Court explains at the outset, the exact question is "whether monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance." *Id.* at 707. In that case, agents had installed a radio transmitter in a can of ether expected to be used in processing cocaine. Without first obtaining a warrant, the agents monitored the signal from the beeper as it moved through a series of residences and multi-unit

storage facilities. *Id.* at 708-09. Where the tracking system enabled the government to locate the can of ether in particular residences, the Supreme Court found that the Fourth Amendment had been infringed. *See id.* at 715 (“The beeper tells the agent a particular article is actually located at a particular time in the private residence [L]ater monitoring ... establishes that the article remains on the premises.”) (emphasis added).

Conversely, the Court found no Fourth Amendment violation where the beeper disclosed only the general location of the ether. In particular, “the beeper equipment was not sensitive enough to allow agents to learn precisely which locker [in the first storage facility] the ether was in.” *Id.* at 708. Instead, the agents learned the can’s precise location inside a specific locker only after subpoenaing the storage company for rental records; tracking the beeper to a specific row of lockers; and then using their sense of smell to detect the ether. *Id.* When one of the targets moved the ether, a similar scenario played out again: agents traced the beeper to another self-storage facility, and then – using their noses – located the smell of ether coming from a given locker. *Id.* at 709.

As to these two episodes, the Supreme Court held emphatically that no Fourth Amendment violation occurred:

[T]he beeper informed the agents only that the ether was somewhere in the warehouse; it did not identify the specific locker in which the ether was located. Monitoring the beeper revealed nothing about the contents of the locker that Horton and Harley had rented and hence was not a search of that locker.

Id. at 720 (emphasis added). In sum, the test under *Karo* is not simply whether a tracked object is inside a private, constitutionally protected pocket, purse, or home. (The can of ether was at the relevant times unquestionably in each of the two lockers, both of which enjoyed a reasonable expectation of privacy. *See id.* n.6.) Rather, *Karo* holds that government use of a tracking device

violates the Fourth Amendment only where the monitoring actually reveals the particular private location in which the tracked object may be found.⁴

The rule in *Karo* conclusively disposes of the Fourth Amendment arguments put forward by amici. As set forth at length in the Government's initial brief, historical cell-site records cannot locate a mobile phone even to within several hundred feet except under optimal conditions. Given that no search occurred in *Karo* when law enforcement tracked the can of ether in real time to a given storage facility or even a specific row of lockers, far less accurate historical cell-site records obtained from a carrier cannot possibly intrude upon a Fourth Amendment privacy interest.⁵

Amici argue unpersuasively that *Karo* bars law enforcement from combining disparate facts (and drawing inferences about location from them) without a warrant. *See* EFF Mem. at 21-23; Freiwald Mem. at 4. But as *Karo* itself makes explicit, the agents in that case were free to use the tracking device to track the beeper to a general area (the storage facility), and then to use a subpoena and their sense of smell to infer the precise location of the can of ether, all without conducting a "search." For the same reasons, law enforcement may obtain historical cell-site records – which do not by themselves disclose the presence of a phone or person within private space – and, by comparing them to other information (such as that derived from visual surveillance), draw additional

⁴Amicus Federal Public Defender argues in its brief that the precision (or lack thereof) of tracking technology is irrelevant to the Fourth Amendment analysis. *See* FPD Mem. at 7 n.4. We respectfully suggest that amicus has overlooked *Karo*'s unequivocal and controlling holding.

⁵For comparable reasons, amicus EFF is mistaken that *Kyllo v. United States*, 533 U.S. 27 (2001), alters this result. *Kyllo* holds that law enforcement may not use infra-red thermal imaging devices to peer through walls and discern activity inside a home without a warrant. That rule is entirely consistent with *Karo*, and therefore imposes no restriction on the government's access to historical cell-site records, which are incapable of revealing activity inside a specific private space.

conclusions. Adopting the contrary rule advocated by amici would make it unlawful even to use a pen register without a warrant, since the information obtained thereby can indicate whether the occupant of a house is making calls (and therefore inside). Because amici's arguments produce such absurd results and openly question well-established Supreme Court precedent,⁶ this Court should reject amici's position and grant the Application.

II. THE 2703(d) STATUTORY STANDARD PROTECTS AGAINST "DRAGNET SURVEILLANCE," AND A COURT MAY NOT IN ITS DISCRETION DEMAND A HIGHER SHOWING OF PROBABLE CAUSE

Amici EFF and Freiwald attempt to portray governmental access to historical cell-site records as "dragnet surveillance" that can be reined in only by requiring a showing of probable cause. EFF Mem. at 24; *see also* Freiwald Mem. at 9. In fact, this melodramatic claim is rebutted by EFF's full-throated advocacy for the very amendment in 1994 that raised the 2703(d) legal standard to its present level requiring "specific and articulable facts."

According to EFF Executive Director Jerry Berman, appearing on August 11, 1994 before a joint House-Senate Judiciary Committee hearing on the pending legislation,

the bill contains a number of significant privacy advances, including enhanced protection for the detailed transactional information records generated by on line [sic] information services, email systems, and the Internet.

1. Expanded protection for transactional records sought by law enforcement

Chief among these new protections is an enhanced protection for transactional records from indiscriminate law enforcement access. ... Provisions in the bill recognize that this transactional information created by new digital communications systems is extremely sensitive and deserves a high degree of protection from casual

⁶*See, e.g.*, EFF Mem. at 19 (openly questioning the holding of *Knotts*).

law enforcement access which is currently possible without any independent judicial supervision. ...

In order to gain access to transactional records ... law enforcement will have to prove to a court, by the showing of "specific and articulable facts" that the records requested are relevant to an ongoing criminal investigation. This means that the government may not request volumes of transactional records merely to see what it can find through traffic analysis. Rather, law enforcement will have to prove to a court that it has reason to believe that it will find specific information relevant to an ongoing criminal investigation in the records it requested. ...

Court order protection will make it much more difficult for law enforcement to go on "fishing expeditions" through online transactional records, hoping to find evidence of a crime by accident. ...

The most important change that these new provisions offer is that law enforcement will: (a) have to convince a judge that there is reason to look at a particular set of records, and; (b) have to expend the time and energy necessary to have a United States Attorney or District Attorney actually present a case before a court.

Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services, 1994: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the Senate Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 103d Cong., 2d Sess. 160-61 (1994) ("Joint CALEA Hearings") (prepared statement of Jerry J. Berman, Executive Director, Electronic Frontier Foundation) (emphasis added).⁷

One month later, EFF offered identical reassurances to a separate House subcommittee. *See Network Wiretapping Capabilities, 1994: Hearings Before the Subcomm. on Telecommunications and Finance of the House Comm. on Energy & Commerce, 103d Cong., 2d Sess. 122-23 (1994)*

⁷A copy of the pertinent excerpts is attached for the Court's convenience as Exhibit A. The full record of the joint hearing is available online at <http://www.lexisnexis.com/congcomp/getdoc?HEARING-ID=HRG-1994-SJS-0015>.

(“House CALEA Hearings”) (prepared statement of Jerry J. Berman, Policy Director, Electronic Frontier Foundation).⁸ And after Congress passed the legislation and transmitted it for the President’s signature, EFF once again hailed the new 2703(d) standard’s robust protection against “indiscriminate access” and “fishing expeditions” by law enforcement. *See EFF Statement on and Analysis of Digital Telephony Act* (Oct. 8, 1994).⁹ Given these repeated claims in zealous support of enacting the current 2703(d) legal standard, amicus EFF cannot now plausibly claim that this same standard permits unchecked “dragnet surveillance.” (Likewise, amicus Federal Public Defender’s hyperbolic invocation of George Orwell’s *1984* – FPD Mem. at 14 – simply does not square with the standard of proof and court oversight demanded by section 2703(d).)

More to the point, the instant Application plainly seeks a limited set of records pertaining to a single individual, offering specific and articulable facts to show that subject’s participation in a drug trafficking conspiracy (and, accordingly, the relevance and materiality of the requested historical cell-site records). Even amicus EFF concedes – albeit grudgingly – that the present Application does not constitute “dragnet surveillance.” *See* EFF Mem. at 24.

Nevertheless, amici argue unconvincingly that ECPA permits a judge to demand probable cause of a 2703(d) applicant, and that denial of the Application was therefore appropriate. Curiously, amici are unable to cite a single case so holding (other than the decision below), nor any supporting discussion in the legislative history, even though the operative language has been present

⁸A version of Berman’s statement (with minor typographic corrections) is available at http://w2.eff.org/Privacy/Surveillance/CALEA/eff_091394_digtel_berman.testimony. The full record of the House hearing is available online at <http://www.lexisnexis.com/congcomp/getdoc?HEARING-ID=HRG-1994-HEC-0049>.

⁹A copy of the EFF statement is available at http://w2.eff.org/Privacy/Surveillance/CALEA/digtel94_passage_statement.eff.

since the enactment of ECPA twenty-two years ago. Further, amici fail to reconcile their position with the statute's structure and history, both of which make clear that 2703(d) orders are a mechanism available to the Government in lieu of obtaining a search warrant. *See* Govt's Mem. at 18-19. The effect of amici's argument is, in short, to read section 2703(d) out of the statute and demand a warrant in its place; because the Fourth Amendment requires no such curative reading, this Court should decline the unwise invitation to nullify section 2703(d).

Here, too, EFF's 1994 declarations in support of raising the 2703(d) standard undercut their present claims. In all three of the documents cited immediately above, EFF's Jerry Berman explicitly represented that "the burden or [sic] proof to be met by the government in such a proceeding [*i.e.*, a 2703(d) application] is lower than required for access to the content of a communication [*i.e.*, probable cause under 2703(a)]." *Joint CALEA Hearings* at 161; *see also House CALEA Hearings* at 123 (verbatim); *EFF Statement on and Analysis of Digital Telephony Act* (verbatim). In short, in its efforts to persuade Congress to raise the 2703(d) standard to its current level – "specific and articulable facts" – EFF publicly and repeatedly acknowledged that 2703(d) applications would not require probable cause. This admission contradicts, and fatally undercuts, EFF's current position that the Government can be required arbitrarily to show probable cause, a claim that in any event finds no support in the body of ECPA case law.

CONCLUSION

For these reasons, the government respectfully submits that this Court should reverse the Opinion and Order below and grant the Application in the instant case.

Respectfully submitted,

MARY BETH BUCHANAN
United States Attorney

s/ Paul E. Hull
PAUL E. HULL
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 894-7311 (Fax)
paul.hull@usdoj.gov
PA ID No. 35302

SOO C. SONG
Assistant U.S. Attorney
U.S. Post Office and Courthouse
700 Grant Street
Suite 4000
Pittsburgh, Pennsylvania 15219
(412) 644-3500 (Phone)
(412) 644-2645 (Fax)
soo.song@usdoj.gov
DC ID No. 457268

MARK ECKENWILER
Associate Director
Office of Enforcement Operations
Criminal Division

U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530

NATHAN JUDISH
Senior Counsel
Computer Crime and Intellectual Property
Section
Criminal Division
U.S. Department of Justice
John Keeney Building
10th Street and Constitution Avenue NW
Washington, DC 20530


The attached forms are for use in obtaining relatively precise location information concerning a wireless phone. It does not refer to "GPS" or "E-911," as those terms are technically inaccurate in describing the location-finding capabilities of many wireless carriers. **Do not use these forms if you want only cell tower/sector records** (sometimes referred to as "cell-site data" or "tower/face information") unless your local judges refuse to grant "hybrid" 3123/2703(d) orders for this less precise class of information.



Note that these forms do not invoke or rely on 18 USC 3117 (the tracking device statute) nor the recently added Rule 41 provisions concerning "tracking devices." This is intentional. The Department's position is that a cell phone knowingly possessed by a user is not a "tracking device" within the meaning of that term as defined in section 3117. However, because a reviewing court might later conclude – contrary to DOJ's view – that a user's own phone falls within the definition, as a precaution these forms include space in the return for indicating when the location-finding activity is first initiated and for what period.

Important considerations in using these forms include

- where to apply: Rule 41(b)(2) permits searches to occur outside the district, provided that the item to be searched is within the district at the time the order is entered. An applicant should determine – whether via information from informants, historical cell tower/sector activity records, or other sources – the probable location of the target phone.

In the alternative, AUSAs may consider invoking 18 USC 2703(c)(1)(A), which permits the compulsion of records from service providers outside the district. OEO disfavors this approach, in part because several courts have rejected the prospective use of 2703. These forms include both options.

-  persons to be notified: OEO recommends giving notice to the person(s) who actually used the target phone, and not merely to the registered owner (if different)

Applicants with additional questions are encouraged to contact the CHIP AUSA in their district or the author of this form (Mark Eckenwiler, Associate Director, Office of Enforcement Operations)  or mark.eckenwiler@doj.gov  **b2**

[DRAFT - Ver. 1.5 2/13/08]

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

UNDER SEAL

AFFIRMATION IN
SUPPORT OF
APPLICATION

STATE OF _____)
COUNTY OF _____ : ss.:
_____ DISTRICT OF _____)

_____, a Special Agent with the _____, being duly
sworn, deposes and states:

INTRODUCTION

1. I am a "federal law enforcement officer" within
the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C),
that is, a government agent engaged in enforcing the criminal
laws and duly authorized by the Attorney General to request a
search warrant. I have been a _____ agent since _____. I have
participated in investigations of _____ and, among other
things, have conducted or participated in surveillances, the
execution of search warrants, debriefings of informants and
reviews of taped conversations. Through my training, education
and experience, I have become familiar with the manner in which
_____.

2. I submit this affidavit in support of an
application for an order pursuant to Federal Rule of Criminal

Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], directing [carrier] to assist agents of the _____ by providing all information, facilities and technical assistance needed to ascertain the physical location of the cellular telephone assigned call number (xxx) xxx-xxxx, with [International Mobile Subscriber Identity /Electronic Serial Number] xxxxxxxxxxxxxxxx, subscribed to in the name _____ at _____ [address]____, with service provided by [carrier] (the "TARGET CELLPHONE"), including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) the TARGET CELLPHONE (the "Requested Information"),¹ for a period of thirty (30) days.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents of the _____ and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and

¹Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records - routinely retained by wireless carriers as business records - may only be obtained via a warrant issued on probable cause. See In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.).

reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another ____ agent, law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

4. Probable cause exists to believe that the Requested Information will lead to evidence of offenses involving _____, in violation of _____ (the "TARGET OFFENSES"), as well as the identification of individuals who are engaged in the commission of these offenses.

5. For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed, are being committed, and will continue to be committed

by _____ and others unknown. [Further, there is probable cause to believe that _____ is using the TARGET CELLPHONE to commit the TARGET OFFENSES.]

Background of the Investigation

6. This application is submitted in connection with a _____ investigation of _____.

7. Based on information obtained from _____, _____ regularly carries the TARGET CELLPHONE [and uses it to conduct illegal activities].

8. The investigation, through, among other things, the use of confidential sources and _____, has revealed, among other things, that _____ and others are engaged in _____.
[Set forth facts tying target cellphone to illegal activities.]

AUTHORIZATION REQUEST

9. Based on the foregoing, there is probable cause to believe that the Requested Information will lead to evidence regarding the activities described above. [OPTIONAL: IF 2703(c)(1)(A) NOT RELIED UPON - SEE COVER INSTRUCTIONS & ¶ 2 & 10 - THEN SET FORTH BASIS FOR BELIEVING THAT TARGET CELLPHONE IS WITHIN THE DISTRICT OF THE ISSUING COURT.] The Requested Information is necessary to determine the approximate location of _____ so that [e.g., law enforcement agents can conduct physical

surveillance of _____ in connection with this expected transaction].

10. WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], it is requested that the Court issue a warrant and Order authorizing the acquisition of the Requested Information and directing [carrier], the service provider for the TARGET CELLPHONE, to initiate a signal to determine the location of the TARGET CELLPHONE on the service provider's network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and to furnish the technical assistance necessary to accomplish the acquisition unobtrusively and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, for a period of thirty (30) days. Reasonable expenses incurred pursuant to this activity will be processed for payment by the _____.

11. IT IS FURTHER REQUESTED that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET CELLPHONE outside of daytime hours.

12. IT IS FURTHER REQUESTED that the warrant and this affirmation, as it reveals an ongoing investigation, be sealed

until further order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that working copies should be made available to the United States Attorney's Office, the ____, and any other law enforcement agency designated by the United States Attorney's Office.

13. IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the monitoring period authorized by the warrant.

Special Agent

Sworn to before me this
____ day of ____ 2008

UNITED STATES MAGISTRATE JUDGE
____ DISTRICT OF _____

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
xxxxxxxxxxxxxxxx

SEALED ORDER

Application having been made by the United States for
an Order pursuant to Federal Rule of Criminal Procedure 41
[OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions],
directing [carrier] to assist agents of the _____ by providing
all information, facilities and technical assistance needed to
ascertain the physical location of the cellular telephone
assigned call number (xxx) xxx-xxxx, with [International Mobile
Subscriber Identity / Electronic Serial Number] xxxxxxxxxxxxxxxxxxxx,
subscribed to in the name _____ at _____ [address] _____, with
service provided by [carrier] (the "TARGET CELLPHONE"), including
but not limited to data indicating the specific latitude and
longitude of (or other precise location information concerning)
the TARGET CELLPHONE (the "Requested Information"), for a period
of thirty (30) days;

The Court finds that there is probable cause to believe that
the Requested Information will lead to evidence of violations of
Title __, United States Code, Sections __ and __, among other

offenses, as well as to the identification of individuals who are engaged in the commission of these offenses.

IT IS HEREBY ORDERED pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions] that [carrier], beginning at any time within ten (10) days of the date of this Order and for a period not to exceed 30 days from the date of this Order, provide to agents of the _____ the Requested Information¹ concerning the TARGET CELLPHONE, with said authority to extend to any time of the day or night as required, including when the TARGET CELLPHONE leaves the _____ District of _____; all of said authority being expressly limited to ascertaining the physical location of the TARGET CELLPHONE and expressly excluding the contents of any communications conducted by the user(s) of the TARGET CELLPHONE.

It is further ORDERED that [carrier], the service provider for the TARGET CELLPHONE, initiate a signal to determine the location of the subject's mobile device on [carrier's] network or with such other reference points as may be reasonably available and at such intervals and times as directed by the law enforcement agent serving the proposed order, and furnish the technical assistance necessary to accomplish the acquisition

¹Such information shall, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call.

unobtrusively and with a minimum of interference with such services as [carrier] accords the user(s) of the TARGET CELLPHONE.

It is further ORDERED that the _____ compensate [carrier] for reasonable expenses incurred in complying with any such request.

It is further ORDERED that the Court's Order and the accompanying Affirmation submitted in support thereof, as they reveal an ongoing investigation, be sealed until further Order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that copies of the Court's Order in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the _____, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and [carrier] as necessary to effectuate the Court's Order.

It is further ORDERED that this warrant be returned to the issuing judicial officer within 10 days after the termination of the execution of the warrant.

It is further ORDERED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of

notice may be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the monitoring period authorized by the warrant.

It is further ORDERED that [carrier], its affiliates, officers, employees, and agents not disclose the Court's Order or the underlying investigation, until notice is given as provided above.

Dated: _____, _____
_____ day of _____ 2008

Time: _____

UNITED STATES MAGISTRATE JUDGE

DISTRICT OF _____

AO
(Rev.
8/97)

WARRANT ON WRITTEN AFFIDAVIT FOR CELL PHONE LOCATION DATA

United States District Court	DISTRICT _____ District of _____	
UNITED STATES OF AMERICA v. PREMISES KNOWN AND DESCRIBED AS A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] XXXXXXXXXXXXXXXXXXXX	DOCKET NO.	MAGISTRATE'S CASE NO.
	To: ANY AUTHORIZED FEDERAL AGENT	
<p>Affidavit having been made before me by the below-named affiant to obtain precise location information concerning the following cell phones (the "Premises"):</p> <p>A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] XXXXXXXXXXXXXXXXXXXX</p> <p>and as I am satisfied that there is good cause for the acquisition of precise location information concerning the Premises,</p> <p>YOU ARE HEREBY COMMANDED to acquire precise location data concerning the Premises named above for a period of thirty (30) days starting within ten (10) calendar days of the date of this order, during any time of day; to return this warrant to the <u>U.S. Magistrate Judge</u> designated in this warrant within ten (10) calendar days after the execution of the warrant has ended; and pursuant to 18 U.S.C. § 3103a(b)(3) authorizing delayed notification, to serve notice within [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] after the monitoring period authorized by the warrant has ended.</p>		
NAME OF AFFIANT Special Agent _____	SIGNATURE OF JUDGE OR U.S. MAGISTRATE	DATE/TIME ISSUED

RETURN

DATE AND TIME ACQUISITION OF LOCATION DATA FIRST INITIATED AND PERIOD DURING WHICH IT WAS ACQUIRED:

CERTIFICATION

I swear that this information contained on this return is true and accurate:

Subscribed, sworn to, and returned before me this date.

Federal Judge or U.S. Magistrate

Date

Eckenwiler, Mark

From: Eckenwiler, Mark
Sent: Friday, November 16, 2007 3:19 PM
To: [REDACTED] b2
Subject: Obtaining prospective, precise location data on wireless phones
Attachments: Generic lat-long order v 1.2 10-07.wpd

CHIPs, I'm writing to repeat the advice given at the CHIP conference in June concerning acquisition of GPS or similarly precise location data (sometimes called "E-911 data") on target phones. We continue to believe that the most appropriate legal mechanism is a Rule 41 warrant, and I'm attaching a sample form for that purpose. (Note: for mere tower/sector data – a/k/a the less accurate "cell-site" records – we remain of the view that 2703(d) & pen/trap combined are sufficient authority.)

To the extent you can, please make your colleagues aware of this recommendation. We continue to hear of applications being made under 2703(d) – sometimes claiming to set forth probable cause – seeking GPS or similarly specific prospective location records, and strongly advise against using this approach in lieu of a Rule 41 warrant.

As always, I welcome your questions, comments, and critiques.

Mark Eckenwiler
Associate Director, OEO
Criminal Division

[REDACTED] b2

The attached forms are for use in obtaining relatively precise location information concerning a wireless phone. It does not refer to "GPS" or "E-911," as those terms are technically inaccurate in describing the location-finding capabilities of many wireless carriers. **Do not use these forms if you want only cell tower/sector records** (sometimes referred to as "cell-site data" or "tower/face information") unless your local judges refuse to grant "hybrid" 3123/2703(d) orders for this less precise class of information.

Note that these forms do not invoke or rely on 18 USC 3117 (the tracking device statute) nor the recently added Rule 41 provisions concerning "tracking devices." This is intentional. The Department's position is that a cell phone knowingly possessed by a user is not a "tracking device" within the meaning of that term as defined in section 3117. However, because a reviewing court might later conclude – contrary to DOJ's view – that a user's own phone falls within the definition, as a precaution these forms include space in the return for indicating when the location-finding activity is first initiated and for what period.

Important considerations in using these forms include

- where to apply: Rule 41(b)(2) permits searches to occur outside the district, provided that the item to be searched is within the district at the time the order is entered. An applicant should determine – whether via information from informants, historical cell tower/sector activity records, or other sources – the probable location of the target phone.

In the alternative, AUSAs may consider invoking 18 USC 2703(c)(1)(A), which permits the compulsion of records from service providers outside the district. OEO disfavors this approach, both because a) several courts have rejected the prospective use of 2703 and b) it is unclear whether location data concerning a user's phone constitutes a "record" in the possession of the provider as contemplated by 2703. These forms include both options.

- persons to be notified: OEO recommends giving notice to the person(s) who actually used the target phone, and not merely to the registered owner (if different)

Applicants with additional questions are encouraged to contact the CHIP AUSA in their district or the author of this form (Mark Eckenwiler, Associate Director, Office of Enforcement Operations, [] or mark.eckenwiler [])

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXX

UNDER SEAL

AFFIRMATION IN
SUPPORT OF
APPLICATION

STATE OF _____)
COUNTY OF _____ : ss.:
_____ DISTRICT OF _____)

_____, a Special Agent with the _____, being duly
sworn, deposes and states:

INTRODUCTION

1. I am a "federal law enforcement officer" within
the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C),
that is, a government agent engaged in enforcing the criminal
laws and duly authorized by the Attorney General to request a
search warrant. I have been a _____ agent since _____. I have
participated in investigations of _____ and, among other
things, have conducted or participated in surveillances, the
execution of search warrants, debriefings of informants and
reviews of taped conversations. Through my training, education
and experience, I have become familiar with the manner in which
_____.

2. I submit this affidavit in support of an
application for an order pursuant to Federal Rule of Criminal

Procedure 41. [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], directing [carrier] to assist agents of the ____ by providing all information, facilities and technical assistance needed to ascertain the physical location of the cellular telephone assigned call number (xxx) xxx-xxxx, with [International Mobile Subscriber Identity /Electronic Serial Number] xxxxxxxxxxxxxxxx, subscribed to in the name _____ at ____ [address] ____, with service provided by [carrier] (the "TARGET CELLPHONE"), including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) the TARGET CELLPHONE (the "Requested Information"),¹ for a period of thirty (30) days.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents of the ____ and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and

¹Such information may, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records - routinely retained by wireless carriers as business records - may only be obtained via a warrant issued on probable cause. See In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.).

reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another ____ agent, law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

4. Probable cause exists to believe that the Requested Information will lead to evidence of offenses involving _____, in violation of _____ (the "TARGET OFFENSES"), as well as the identification of individuals who are engaged in the commission of these offenses.

5. For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed, are being committed, and will continue to be committed

by _____ and others unknown. [Further, there is probable cause to believe that _____ is using the TARGET CELLPHONE to commit the TARGET OFFENSES.]

Background of the Investigation

6. This application is submitted in connection with a _____ investigation of _____.

7. Based on information obtained from _____, _____ regularly carries the TARGET CELLPHONE [and uses it to conduct illegal activities].

8. The investigation, through, among other things, the use of confidential sources and _____, has revealed, among other things, that _____ and others are engaged in _____.
[Set forth facts tying target cellphone to illegal activities.]

AUTHORIZATION REQUEST

9. Based on the foregoing, there is probable cause to believe that the Requested Information will lead to evidence regarding the activities described above. [OPTIONAL: IF 2703(c)(1)(A) NOT RELIED UPON - SEE COVER INSTRUCTIONS & §§ 2 & 10 - THEN SET FORTH BASIS FOR BELIEVING THAT TARGET CELLPHONE IS WITHIN THE DISTRICT OF THE ISSUING COURT.] The Requested Information is necessary to determine the approximate location of _____ so that [e.g., law enforcement agents can conduct physical

surveillance of _____ in connection with this expected transaction].

10. WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], it is requested that the Court issue a warrant and Order authorizing the acquisition of the Requested Information and directing [carrier], the service provider for the TARGET CELLPHONE, to furnish the technical assistance necessary to accomplish the acquisition unobtrusively, and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, for a period of thirty (30) days. Reasonable expenses incurred pursuant to this activity will be processed for payment by the _____.

11. IT IS FURTHER REQUESTED that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET CELLPHONE outside of daytime hours.

12. IT IS FURTHER REQUESTED that the warrant and this affirmation, as it reveals an ongoing investigation, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that working copies should be made available to the United States

Attorney's Office, the ____, and any other law enforcement agency designated by the United States Attorney's Office.

13. IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the execution of the warrant.

Special Agent

Sworn to before me this
__ day of ____ 2007

UNITED STATES MAGISTRATE JUDGE
____ DISTRICT OF _____

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
xxxxxxxxxxxxxxxxxx

SEALED ORDER

Application having been made by the United States for
an Order pursuant to Federal Rule of Criminal Procedure 41
[OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions],
directing [carrier] to assist agents of the _____ by providing
all information, facilities and technical assistance needed to
ascertain the physical location of the cellular telephone
assigned call number (xxx) xxx-xxxx, with [International Mobile
Subscriber Identity / Electronic Serial Number] xxxxxxxxxxxxxxxxxxxx,
subscribed to in the name _____ at _____ [address] _____, with
service provided by [carrier] (the "TARGET CELLPHONE"), including
but not limited to data indicating the specific latitude and
longitude of (or other precise location information concerning)
the TARGET CELLPHONE (the "Requested Information"), for a period
of thirty (30) days;

The Court finds that there is probable cause to believe that
the Requested Information will lead to evidence of violations of
Title __, United States Code, Sections ____ and ____, among other

offenses, as well as to the identification of individuals who are engaged in the commission of these offenses.

IT IS HEREBY ORDERED pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions] that [carrier], beginning at any time within ten (10) days of the date of this Order and for a period not to exceed 30 days from the date of this Order, provide to agents of the _____ the Requested Information concerning the TARGET CELLPHONE, with said authority to extend to any time of the day or night as required, including when the TARGET CELLPHONE leaves the _____ District of _____; all of said authority being expressly limited to ascertaining the physical location of the TARGET CELLPHONE and expressly excluding the contents of any communications conducted by the user(s) of the TARGET CELLPHONE.

It is further ORDERED that the _____ compensate [carrier] for reasonable expenses incurred in complying with any such request.

It is further ORDERED that agents of the _____ and other law enforcement officers and persons authorized to provide them with necessary and technical assistance are authorized to acquire the Requested Information concerning the location of the TARGET CELLPHONE for a period of thirty (30) days from the date of this Order or until the goals of the investigation have been achieved.

It is further ORDERED that the Court's Order and the accompanying Affirmation submitted in support thereof, as they

reveal an ongoing investigation, be sealed until further Order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that copies of the Court's Order in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the _____, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and [carrier] as necessary to effectuate the Court's Order.

It is further ORDERED that this warrant be returned to the issuing judicial officer within 10 days after the termination of the execution of the warrant.

It is further ORDERED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of notice may be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the execution of the warrant.

It is further ORDERED that [carrier], its affiliates, officers, employees, and agents not disclose the Court's Order or the underlying investigation, until notice is given as provided above.

Dated: _____, _____ day of _____ 2007

Time: _____

UNITED STATES MAGISTRATE JUDGE
DISTRICT OF _____

AO
(Rev.
8/97)

WARRANT ON WRITTEN AFFIDAVIT FOR CELL PHONE LOCATION DATA

United States District Court	DISTRICT _____ District of _____	
UNITED STATES OF AMERICA v. PREMISES KNOWN AND DESCRIBED AS A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] XXXXXXXXXXXXXXXXXXXX	DOCKET NO.	MAGISTRATE'S CASE NO.
	To: ANY AUTHORIZED FEDERAL AGENT	
<p>Affidavit having been made before me by the below-named affiant to obtain precise location information concerning the following cell phones (the "Premises"):</p> <p>A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] XXXXXXXXXXXXXXXXXXXX</p> <p>and as I am satisfied that there is good cause for the acquisition of precise location information concerning the Premises,</p> <p>YOU ARE HEREBY COMMANDED to acquire precise location data concerning the Premises named above for a period of thirty (30) days starting within ten (10) calendar days of the date of this order, during any time of day; to return this warrant to the <u>U.S. Magistrate Judge</u> designated in this warrant within ten (10) calendar days after the execution of the warrant has ended; and pursuant to 18 U.S.C. § 3103a(b)(3) authorizing delayed notification, to serve notice within [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] after the execution of the warrant has ended.</p>		
NAME OF AFFIANT Special Agent _____	SIGNATURE OF JUDGE OR U.S. MAGISTRATE	DATE/TIME ISSUED

RETURN

DATE AND TIME ACQUISITION OF LOCATION DATA FIRST INITIATED AND PERIOD DURING WHICH IT WAS ACQUIRED:

CERTIFICATION

I swear that this information contained on this return is true and accurate:

Subscribed, sworn to, and returned before me this date.

Federal Judge or U.S. Magistrate

Date

REFERRALS FROM EOUSA

No. 07-4132

No. 07-4129

Liebermann, Erez (USANJ)

07-4132

From: [redacted] on behalf of Eckenwiler, Mark (CRM)
Sent: Friday, September 12, 2008 2:38 PM
To: USAEO-CrimChiefs
Cc: [redacted]
Subject: [chip] OEO guidance concerning requests for historical cellular telephone location information
Attachments: Final Memorandum of Law (WDPA).pdf; Exhibit C.PDF; reply -- final as filed.pdf

To: All USAO Criminal Chiefs

From: Office of Enforcement Operations, Criminal Division

Re: Guidance Concerning Requests for Historical Cellular Telephone Location Information

Date: September 12, 2008

A number of offices have inquired about a decision earlier this week from the District Court in W.D. Pa. that has received widespread press coverage. In the expectation that many of your local magistrate judges will be relying on this opinion, I am writing to offer guidance.

The case involves a request by the U.S. Attorney's Office in Pittsburgh for the wireless phone records of a suspected narcotics trafficker. The USAO sought to obtain cell-site records – that is, records showing the tower and tower face used at the start and end of calls – for a specified time period in the past, basing its request on 18 USC 2703(d) (requiring a showing of “specific and articulable facts,” a standard lower than probable cause).

Without requesting briefing on the law or the underlying technology, the magistrate judge (joined by four fellow magistrates) issued a lengthy opinion in February 2008 holding that such records may not be obtained absent a search warrant based upon probable cause. *See In re Application*, 534 F. Supp. 2d 585 (W.D. Pa. 2008). The USAO promptly appealed, only to have the district court summarily affirm in a two-page decision on Wednesday of this week.

As indicated in the attached opening brief and reply, we believe that both decisions are wrong on the facts as well as the law. Most importantly, the magistrate wrongly analyzed the request under the law governing prospective location surveillance, notwithstanding the fact that the USAO requested only historical records. In addition, the published opinion materially misstates the degree of precision of the requested records, conflating cell-site records – indicating the user's location at best only to within hundreds of yards – with more precise location information (such as GPS coordinates, typically unavailable for past periods). Both the magistrates and the district court ignored previous decisions in other districts explicitly endorsing the Department's position that historical tower/sector records may be compelled using a section 2703(d) order. *See In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007); *In re Application*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007). The USAO, in consultation with Criminal Division, is considering its options for seeking further judicial review.

Where agents seek to obtain GPS (or similarly precise) information for a target's phone on a prospective basis, OEO continues to recommend the use of a warrant under Rule 41. (Regularly updated model forms, either for standalone use or in connection with a Title III application, are available on request.) However, we remain firmly of the view that access to less-precise historical cell-site records, routinely kept by providers in the ordinary course of business, is governed by section 2703(d) and does not require a search warrant.

If you have any questions, or encounter difficulty on this issue with judges in your own district, please do not hesitate to contact me.

Mark Eckenwiler
Associate Director
Office of Enforcement Operations
Criminal Division

The attached forms are for use in obtaining relatively precise location information concerning a wireless phone. It does not refer to "GPS" or "E-911," as those terms are technically inaccurate in describing the location-finding capabilities of many wireless carriers. **Do not use these forms if you want only cell tower/sector records** (sometimes referred to as "cell-site data" or "tower/face information") unless your local judges refuse to grant "hybrid" 3123/2703(d) orders for this less precise class of information.

Note that these forms do not invoke or rely on 18 USC 3117 (the tracking device statute) nor the recently added Rule 41 provisions concerning "tracking devices." This is intentional. The Department's position is that a cell phone knowingly possessed by a user is not a "tracking device" within the meaning of that term as defined in section 3117. However, because a reviewing court might later conclude – contrary to DOJ's view – that a user's own phone falls within the definition, as a precaution these forms include space in the return for indicating when the location-finding activity is first initiated and for what period.

Important considerations in using these forms include

- where to apply: Rule 41(b)(2) permits searches to occur outside the district, provided that the item to be searched is within the district at the time the order is entered. An applicant should determine – whether via information from informants, historical cell tower/sector activity records, or other sources – the probable location of the target phone.

In the alternative, AUSAs may consider invoking 18 USC 2703(c)(1)(A), which permits the compulsion of records from service providers outside the district. OEO disfavors this approach, both because a) several courts have rejected the prospective use of 2703 and b) it is unclear whether location data concerning a user's phone constitutes a "record" in the possession of the provider as contemplated by 2703. These forms include both options.

[] b5

- persons to be notified: OEO recommends giving notice to the person(s) who actually used the target phone, and not merely to the registered owner (if different)

Applicants with additional questions are encouraged to contact the CHIP AUSA in their district or the author of this form (Mark Eckenwiler, Associate Director, Office of Enforcement Operations, [] or mark.eckenwiler [] b2

[DRAFT - Ver. 1.2 10/25/07]

duplicate (10/25/07)
referred
CPM

UNITED STATES DISTRICT COURT
DISTRICT OF _____

duplicates
CRM RIF
08/22/08

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

UNDER SEAL

AFFIRMATION IN
SUPPORT OF
APPLICATION

STATE OF _____)
COUNTY OF _____ : ss.:
_____ DISTRICT OF _____)

_____, a Special Agent with the _____, being duly
sworn, deposes and states:

INTRODUCTION

1. I am a "federal law enforcement officer" within
the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C),
that is, a government agent engaged in enforcing the criminal
laws and duly authorized by the Attorney General to request a
search warrant. I have been a _____ agent since _____. I have
participated in investigations of _____ and, among other
things, have conducted or participated in surveillances, the
execution of search warrants, debriefings of informants and
reviews of taped conversations. Through my training, education
and experience, I have become familiar with the manner in which
_____.

2. I submit this affidavit in support of an
application for an order pursuant to Federal Rule of Criminal

Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], directing [carrier] to assist agents of the _____ by providing all information, facilities and technical assistance needed to ascertain the physical location of the cellular telephone assigned call number (xxx) xxx-xxxx, with [International Mobile Subscriber Identity /Electronic Serial Number] xxxxxxxxxxxxxxxxx, subscribed to in the name _____ at _____ [address]____, with service provided by [carrier] (the "TARGET CELLPHONE"), including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) the TARGET CELLPHONE (the "Requested Information"),¹ for a period of thirty (30) days.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents of the _____ and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and

¹Such information may, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records - routinely retained by wireless carriers as business records - may only be obtained via a warrant issued on probable cause. See In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.).

reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another ____ agent, law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

4. Probable cause exists to believe that the Requested Information will lead to evidence of offenses involving _____, in violation of _____ (the "TARGET OFFENSES"), as well as the identification of individuals who are engaged in the commission of these offenses.

5. For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed, are being committed, and will continue to be committed

by _____ and others unknown. [Further, there is probable cause to believe that _____ is using the TARGET CELLPHONE to commit the TARGET OFFENSES.]

Background of the Investigation

6. This application is submitted in connection with a _____ investigation of _____.

7. Based on information obtained from _____, _____ regularly carries the TARGET CELLPHONE [and uses it to conduct illegal activities].

8. The investigation, through, among other things, the use of confidential sources and _____, has revealed, among other things, that _____ and others are engaged in _____.
[Set forth facts tying target cellphone to illegal activities.]

AUTHORIZATION REQUEST

9. Based on the foregoing, there is probable cause to believe that the Requested Information will lead to evidence regarding the activities described above. [OPTIONAL: IF 2703(c)(1)(A) NOT RELIED UPON - SEE COVER INSTRUCTIONS & ¶¶ 2 & 10 - THEN SET FORTH BASIS FOR BELIEVING THAT TARGET CELLPHONE IS WITHIN THE DISTRICT OF THE ISSUING COURT.] The Requested Information is necessary to determine the approximate location of _____ so that [e.g., law enforcement agents can conduct physical

surveillance of _____ in connection with this expected transaction].

10. WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], it is requested that the Court issue a warrant and Order authorizing the acquisition of the Requested Information and directing [carrier], the service provider for the TARGET CELLPHONE, to furnish the technical assistance necessary to accomplish the acquisition unobtrusively, and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, for a period of thirty (30) days. Reasonable expenses incurred pursuant to this activity will be processed for payment by the _____.

11. IT IS FURTHER REQUESTED that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET CELLPHONE outside of daytime hours.

12. IT IS FURTHER REQUESTED that the warrant and this affirmation, as it reveals an ongoing investigation, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that working copies should be made available to the United States

Attorney's Office, the ____, and any other law enforcement agency designated by the United States Attorney's Office.

13. IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the execution of the warrant.

Special Agent

Sworn to before me this
____ day of ____ 2007

UNITED STATES MAGISTRATE JUDGE
____ DISTRICT OF _____

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
xxxxxxxxxxxxxxxxxxxx

SEALED ORDER

Application having been made by the United States for
an Order pursuant to Federal Rule of Criminal Procedure 41
[OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions],
directing [carrier] to assist agents of the _____ by providing
all information, facilities and technical assistance needed to
ascertain the physical location of the cellular telephone
assigned call number (xxx) xxx-xxxx, with [International Mobile
Subscriber Identity / Electronic Serial Number] xxxxxxxxxxxxxxxx,
subscribed to in the name _____ at _____ [address] _____, with
service provided by [carrier] (the "TARGET CELLPHONE"), including
but not limited to data indicating the specific latitude and
longitude of (or other precise location information concerning)
the TARGET CELLPHONE (the "Requested Information"), for a period
of thirty (30) days;

The Court finds that there is probable cause to believe that
the Requested Information will lead to evidence of violations of
Title __, United States Code, Sections ____ and ____, among other

offenses, as well as to the identification of individuals who are engaged in the commission of these offenses.

IT IS HEREBY ORDERED pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions] that [carrier], beginning at any time within ten (10) days of the date of this Order and for a period not to exceed 30 days from the date of this Order, provide to agents of the _____ the Requested Information concerning the TARGET CELLPHONE, with said authority to extend to any time of the day or night as required, including when the TARGET CELLPHONE leaves the _____ District of _____; all of said authority being expressly limited to ascertaining the physical location of the TARGET CELLPHONE and expressly excluding the contents of any communications conducted by the user(s) of the TARGET CELLPHONE.

It is further ORDERED that the _____ compensate [carrier] for reasonable expenses incurred in complying with any such request.

It is further ORDERED that agents of the _____ and other law enforcement officers and persons authorized to provide them with necessary and technical assistance are authorized to acquire the Requested Information concerning the location of the TARGET CELLPHONE for a period of thirty (30) days from the date of this Order or until the goals of the investigation have been achieved.

It is further ORDERED that the Court's Order and the accompanying Affirmation submitted in support thereof, as they

reveal an ongoing investigation, be sealed until further Order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that copies of the Court's Order in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the ___, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and [carrier] as necessary to effectuate the Court's Order.

It is further ORDERED that this warrant be returned to the issuing judicial officer within 10 days after the termination of the execution of the warrant.

It is further ORDERED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of notice may be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the execution of the warrant.

It is further ORDERED that [carrier], its affiliates, officers, employees, and agents not disclose the Court's Order or the underlying investigation, until notice is given as provided above.

Dated: _____, _____ day of _____ 2007

Time: _____

UNITED STATES MAGISTRATE JUDGE
____ DISTRICT OF _____

AO

(Rev.
8/97)

WARRANT ON WRITTEN AFFIDAVIT FOR CELL PHONE LOCATION DATA

<i>United States District Court</i>	DISTRICT _____ District of _____	
UNITED STATES OF AMERICA v. PREMISES KNOWN AND DESCRIBED AS A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] XXXXXXXXXXXXXXXXXXXX	DOCKET NO.	MAGISTRATE'S CASE NO.
	To: ANY AUTHORIZED FEDERAL AGENT	
<p>Affidavit having been made before me by the below-named affiant to obtain precise location information concerning the following cell phones (the "Premises"):</p> <p>A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH [INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER] XXXXXXXXXXXXXXXXXXXX</p> <p>and as I am satisfied that there is good cause for the acquisition of precise location information concerning the Premises,</p> <p>YOU ARE HEREBY COMMANDED to acquire precise location data concerning the Premises named above for a period of thirty (30) days starting within ten (10) calendar days of the date of this order, during any time of day; to return this warrant to the <u>U.S. Magistrate Judge</u> designated in this warrant within ten (10) calendar days after the execution of the warrant has ended; and pursuant to 18 U.S.C. § 3103a(b)(3) authorizing delayed notification, to serve notice within [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] after the execution of the warrant has ended.</p>		
NAME OF AFFIANT Special Agent _____	SIGNATURE OF JUDGE OR U.S. MAGISTRATE	DATE/TIME ISSUED

RETURN

DATE AND TIME ACQUISITION OF LOCATION DATA FIRST INITIATED AND PERIOD DURING WHICH IT WAS ACQUIRED:

CERTIFICATION

I swear that this information contained on this return is true and accurate:

Subscribed, sworn to, and returned before me this date.

Federal Judge or U.S. Magistrate

Date

The attached forms are for use in obtaining relatively precise location information concerning a wireless phone. It does not refer to "GPS" or "E-911," as those terms are technically inaccurate in describing the location-finding capabilities of many wireless carriers. Do not use these forms if you want only cell tower/sector records (sometimes referred to as "cell-site data" or "tower/face information") unless your local judges refuse to grant "hybrid" 3123/2703(d) orders for this less precise class of information.

Note that these forms do not invoke or rely on 18 USC 3117 (the tracking device statute) nor the recently added Rule 41 provisions concerning "tracking devices." This is intentional. The Department's position is that a cell phone knowingly possessed by a user is not a "tracking device" within the meaning of that term as defined in section 3117. However, because a reviewing court might later conclude – contrary to DOJ's view – that a user's own phone falls within the definition, as a precaution these forms include space in the return for indicating when the location-finding activity is first initiated and for what period.

Important considerations in using these forms include

- where to apply: Rule 41(b)(2) permits searches to occur outside the district, provided that the item to be searched is within the district at the time the order is entered. An applicant should determine – whether via information from informants, historical cell tower/sector activity records, or other sources – the probable location of the target phone.

In the alternative, AUSAs may consider invoking 18 USC 2703(c)(1)(A), which permits the compulsion of records from service providers outside the district. OEO disfavors this approach, both because a) several courts have rejected the prospective use of 2703 and b) it is unclear whether location data concerning a user's phone constitutes a "record" in the possession of the provider as contemplated by 2703. These forms include both options.

[] b5

- persons to be notified: OEO recommends giving notice to the person(s) who actually used the target phone, and not merely to the registered owner (if different)

Applicants with additional questions are encouraged to contact the CHIP AUSA in their district or the author of this form (Mark Eckenwiler, Associate Director, Office of Enforcement Operations, [] or mark.eckenwiler []).

[DRAFT - Ver. 1.2 10/25/07] b2

UNITED STATES DISTRICT COURT
DISTRICT OF _____

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

UNDER SEAL

AFFIRMATION IN
SUPPORT OF
APPLICATION

STATE OF _____)
COUNTY OF _____ : ss.:
_____ DISTRICT OF _____)

_____, a Special Agent with the _____, being duly
sworn, deposes and states:

INTRODUCTION

1. I am a "federal law enforcement officer" within
the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C),
that is, a government agent engaged in enforcing the criminal
laws and duly authorized by the Attorney General to request a
search warrant. I have been a _____ agent since _____. I have
participated in investigations of _____ and, among other
things, have conducted or participated in surveillances, the
execution of search warrants, debriefings of informants and
reviews of taped conversations. Through my training, education
and experience, I have become familiar with the manner in which
_____.

2. I submit this affidavit in support of an
application for an order pursuant to Federal Rule of Criminal

Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c) (1) (A)] [see cover instructions], directing [carrier] to assist agents of the ____ by providing all information, facilities and technical assistance needed to ascertain the physical location of the cellular telephone assigned call number (xxx) xxx-xxxx, with [International Mobile Subscriber Identity /Electronic Serial Number] xxxxxxxxxxxxxxxx, subscribed to in the name _____ at _____[address]____, with service provided by [carrier] (the "TARGET CELLPHONE"), including but not limited to data indicating the specific latitude and longitude of (or other precise location information concerning) the TARGET CELLPHONE (the "Requested Information"),¹ for a period of thirty (30) days.

3. I have personally participated in the investigation set forth below. I am familiar with the facts and circumstances of the investigation through my personal participation; from discussions with other agents of the ____ and other law enforcement; from my discussions with witnesses involved in the investigation; and from my review of records and

¹Such information may, where other information is unavailable, include records reflecting the tower and antenna face ("cell site") used by the TARGET CELLPHONE at the start and end of any call. In requesting cell site information, the Government does not concede that such cell site records - routinely retained by wireless carriers as business records - may only be obtained via a warrant issued on probable cause. See In re Application, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (authorizing prospective acquisition of cell-site records under combined authority of 18 U.S.C. 2703(d) & 3121 et seq.).

reports relating to the investigation. Unless otherwise noted, wherever in this affidavit I assert that a statement was made, the information was provided by another ____ agent, law enforcement officer or witness who may have had either direct or hearsay knowledge of that statement and to whom I or others have spoken or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this affidavit is being submitted for the limited purpose of securing an order authorizing the acquisition of the Requested Information, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied on in reaching my conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

4. Probable cause exists to believe that the Requested Information will lead to evidence of offenses involving _____, in violation of _____ (the "TARGET OFFENSES"), as well as the identification of individuals who are engaged in the commission of these offenses.

5. For the reasons set out in this affidavit, there is probable cause to believe that the TARGET OFFENSES have been committed, are being committed, and will continue to be committed

by _____ and others unknown. [Further, there is probable cause to believe that _____ is using the TARGET CELLPHONE to commit the TARGET OFFENSES.]

Background of the Investigation

6. This application is submitted in connection with a _____ investigation of _____.

7. Based on information obtained from _____, _____ regularly carries the TARGET CELLPHONE [and uses it to conduct illegal activities].

8. The investigation, through, among other things, the use of confidential sources and _____, has revealed, among other things, that _____ and others are engaged in _____.
[Set forth facts tying target cellphone to illegal activities.]

AUTHORIZATION REQUEST

9. Based on the foregoing, there is probable cause to believe that the Requested Information will lead to evidence regarding the activities described above. [OPTIONAL: IF 2703(c)(1)(A) NOT RELIED UPON - SEE COVER INSTRUCTIONS & ¶ 2 & 10 - THEN SET FORTH BASIS FOR BELIEVING THAT TARGET CELLPHONE IS WITHIN THE DISTRICT OF THE ISSUING COURT.] The Requested Information is necessary to determine the approximate location of _____ so that [e.g., law enforcement agents can conduct physical

surveillance of _____ in connection with this expected transaction].

10. WHEREFORE, pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions], it is requested that the Court issue a warrant and Order authorizing the acquisition of the Requested Information and directing [carrier], the service provider for the TARGET CELLPHONE, to furnish the technical assistance necessary to accomplish the acquisition unobtrusively, and with a minimum of interference with such services as that provider accords the user(s) of the TARGET CELLPHONE, for a period of thirty (30) days. Reasonable expenses incurred pursuant to this activity will be processed for payment by the _____.

11. IT IS FURTHER REQUESTED that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the TARGET CELLPHONE outside of daytime hours.

12. IT IS FURTHER REQUESTED that the warrant and this affirmation, as it reveals an ongoing investigation, be sealed until further order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that working copies should be made available to the United States

Attorney's Office, the _____, and any other law enforcement agency designated by the United States Attorney's Office.

13. IT IS FURTHER REQUESTED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), the Court authorize notice to be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the execution of the warrant.

Special Agent

Sworn to before me this
____ day of ____ 2007

UNITED STATES MAGISTRATE JUDGE
____ DISTRICT OF _____

UNITED STATES DISTRICT COURT
DISTRICT OF

IN THE MATTER OF THE APPLICATION
OF THE UNITED STATES OF AMERICA
FOR AUTHORIZATION TO OBTAIN LOCATION
DATA CONCERNING A CELLULAR TELEPHONE
ASSIGNED CALL NUMBER (xxx) xxx-xxxx,
WITH [INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

SEALED ORDER

Application having been made by the United States for
an Order pursuant to Federal Rule of Criminal Procedure 41
[OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions],
directing [carrier] to assist agents of the _____ by providing
all information, facilities and technical assistance needed to
ascertain the physical location of the cellular telephone
assigned call number (xxx) xxx-xxxx, with [International Mobile
Subscriber Identity / Electronic Serial Number] xxxxxxxxxxxxxxxx,
subscribed to in the name _____ at _____ [address] _____, with
service provided by [carrier] (the "TARGET CELLPHONE"), including
but not limited to data indicating the specific latitude and
longitude of (or other precise location information concerning)
the TARGET CELLPHONE (the "Requested Information"), for a period
of thirty (30) days;

The Court finds that there is probable cause to believe that
the Requested Information will lead to evidence of violations of
Title __, United States Code, Sections __ and __, among other

offenses, as well as to the identification of individuals who are engaged in the commission of these offenses.

IT IS HEREBY ORDERED pursuant to Federal Rule of Criminal Procedure 41 [OPTIONAL: and 18 U.S.C. 2703(c)(1)(A)] [see cover instructions] that [carrier], beginning at any time within ten (10) days of the date of this Order and for a period not to exceed 30 days from the date of this Order, provide to agents of the _____ the Requested Information concerning the TARGET CELLPHONE, with said authority to extend to any time of the day or night as required, including when the TARGET CELLPHONE leaves the _____ District of _____; all of said authority being expressly limited to ascertaining the physical location of the TARGET CELLPHONE and expressly excluding the contents of any communications conducted by the user(s) of the TARGET CELLPHONE.

It is further ORDERED that the _____ compensate [carrier] for reasonable expenses incurred in complying with any such request.

It is further ORDERED that agents of the _____ and other law enforcement officers and persons authorized to provide them with necessary and technical assistance are authorized to acquire the Requested Information concerning the location of the TARGET CELLPHONE for a period of thirty (30) days from the date of this Order or until the goals of the investigation have been achieved.

It is further ORDERED that the Court's Order and the accompanying Affirmation submitted in support thereof, as they

reveal an ongoing investigation, be sealed until further Order of the Court in order to avoid premature disclosure of the investigation, guard against fugitives, and better ensure the safety of agents and others, except that copies of the Court's Order in full or redacted form may be maintained by the United States Attorney's Office, and may be served on Special Agents and other investigative and law enforcement officers of the ___, federally deputized state and local law enforcement officers, and other government and contract personnel acting under the supervision of such investigative or law enforcement officers, and [carrier] as necessary to effectuate the Court's Order.

It is further ORDERED that this warrant be returned to the issuing judicial officer within 10 days after the termination of the execution of the warrant.

It is further ORDERED that, pursuant to 18 U.S.C. 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), service of notice may be delayed for a period of [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] days after the termination of the execution of the warrant.

It is further ORDERED that [carrier], its affiliates, officers, employees, and agents not disclose the Court's Order or the underlying investigation, until notice is given as provided above.

Dated: _____, _____
_____ day of _____ 2007

Time: _____

UNITED STATES MAGISTRATE JUDGE
____ DISTRICT OF _____

AO
(Rev.
8/97)

WARRANT ON WRITTEN AFFIDAVIT FOR CELL PHONE LOCATION DATA

United States District Court

DISTRICT

____ District of ____

UNITED STATES OF AMERICA

v.

DOCKET NO.

MAGISTRATE'S CASE NO.

To:

ANY AUTHORIZED FEDERAL AGENT

PREMISES KNOWN AND DESCRIBED AS
A CELLULAR TELEPHONE ASSIGNED CALL
NUMBER (xxx) xxx-xxxx, WITH
[INTERNATIONAL MOBILE SUBSCRIBER
IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

Affidavit having been made before me by the below-named affiant to obtain precise location information concerning the following cell phones (the "Premises"):

A CELLULAR TELEPHONE ASSIGNED CALL NUMBER (xxx) xxx-xxxx, WITH
[INTERNATIONAL MOBILE SUBSCRIBER IDENTITY / ELECTRONIC SERIAL NUMBER]
XXXXXXXXXXXXXXXXXXXX

and as I am satisfied that there is good cause for the acquisition of precise location information concerning the Premises,

YOU ARE HEREBY COMMANDED to acquire precise location data concerning the Premises named above for a period of thirty (30) days starting within ten (10) calendar days of the date of this order, during any time of day; to return this warrant to the U.S. Magistrate Judge designated in this warrant within ten (10) calendar days after the execution of the warrant has ended; and pursuant to 18 U.S.C. § 3103a(b)(3) authorizing delayed notification, to serve notice within [INSERT NUMBER NO GREATER THAN 30; SEE ALSO COVER SHEET] after the execution of the warrant has ended.

NAME OF AFFIANT

SIGNATURE OF JUDGE OR U.S. MAGISTRATE

DATE/TIME ISSUED

Special Agent _____

RETURN

DATE AND TIME ACQUISITION OF LOCATION DATA FIRST INITIATED AND PERIOD DURING WHICH IT WAS ACQUIRED:

CERTIFICATION

I swear that this information contained on this return is true and accurate:

Subscribed, sworn to, and returned before me this date.

Federal Judge or U.S. Magistrate

Date

EUSA e-mails

From: Eckenwiler, Mark (CRM)
To: USAEO-CrimChiefs
Cc: [redacted] b2
Sent: Fri Sep 12 14:37:31 2008
Subject: OEO guidance concerning requests for historical cellular telephone location information
To: All USAO Criminal Chiefs

From: Office of Enforcement Operations, Criminal Division

Re: Guidance Concerning Requests for Historical Cellular Telephone Location Information

Date: September 12, 2008

A number of offices have inquired about a decision earlier this week from the District Court in W.D. Pa. that has received widespread press coverage. In the expectation that many of your local magistrate judges will be relying on this opinion, I am writing to offer guidance.

The case involves a request by the U.S. Attorney's Office in Pittsburgh for the wireless phone records of a suspected narcotics trafficker. The USAO sought to obtain cell-site records – that is, records showing the tower and tower face used at the start and end of calls – for a specified time period in the past, basing its request on 18 USC 2703(d) (requiring a showing of “specific and articulable facts,” a standard lower than probable cause).

Without requesting briefing on the law or the underlying technology, the magistrate judge (joined by four fellow magistrates) issued a lengthy opinion in February 2008 holding that such records may not be obtained absent a search warrant based upon probable cause. *See In re Application*, 534 F. Supp. 2d 585 (W.D. Pa.

2008). The USAO promptly appealed, only to have the district court summarily affirm in a two-page decision on Wednesday of this week.

As indicated in the attached opening brief and reply, we believe that both decisions are wrong on the facts as well as the law. Most importantly, the magistrate wrongly analyzed the request under the law governing prospective location surveillance, notwithstanding the fact that the USAO requested only historical records. In addition, the published opinion materially misstates the degree of precision of the requested records, conflating cell-site records – indicating the user's location at best only to within hundreds of yards – with more precise location information (such as GPS coordinates, typically unavailable for past periods). Both the magistrates and the district court ignored previous decisions in other districts explicitly endorsing the Department's position that historical tower/sector records may be compelled using a section 2703(d) order. *See In re Applications*, 509 F. Supp. 2d 76 (D. Mass. 2007); *In re Application*, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007). The USAO, in consultation with Criminal Division, is considering its options for seeking further judicial review.

Where agents seek to obtain GPS (or similarly precise) information for a target's phone on a prospective basis, OEO continues to recommend the use of a warrant under Rule 41. (Regularly updated model forms, either for standalone use or in connection with a Title III application, are available on request.) However, we remain firmly of the view that access to less-precise historical cell-site records, routinely kept by providers in the ordinary course of business, is governed by section 2703(d) and does not require a search warrant.

If you have any questions, or encounter difficulty on this issue with judges in your own district, please do not hesitate to contact me.

Mark Eckenwiler
Associate Director
Office of Enforcement Operations
Criminal Division