No.08-4227

IN THE UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

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

Appeal from Memorandum Order Entered by the United States District Court for the Western District of Pennsylvania (McVerry, J.) at Magistrate No. 07-524M

BRIEF FOR THE UNITED STATES

MARY BETH BUCHANAN United States Attorney

Robert L. Eberhardt Assistant U.S. Attorney

Mark Eckenwiler Associate Director United States Department of Justice Office of Enforcement Operations Criminal Division

700 Grant Street, Suite 4000 Pittsburgh, Pennsylvania 15219

Tel: (412) 894-7353 Fax: (412) 644-5870

E-Mail: Robert.Eberhardt@usdoj.gov

TABLE OF CONTENTS

<u>Page</u>	S
TABLE OF CITATIONS i	i
JURISDICTION	1
ISSUES PRESENTED	2
STANDARDS OF REVIEW	2
STATEMENT OF RELATED PROCEEDINGS	3
STATEMENT OF THE CASE	4
SUMMARY OF ARGUMENT	7
ARGUMENT	
I. THE GOVERNMENT MAY COMPEL A WIRELESS SERVICE PROVIDER TO DISCLOSE HISTORICAL CELL-SITE RECORDS PERTAINING TO A SUBSCRIBER BY MEANS OF A COURT ORDER ISSUED UNDER 18 U.S.C. § 2703(d)	8
II. THE FOURTH AMENDMENT DOES NOT BAR COMPELLED DISCLOSURE OF HISTORICAL CELL-SITE INFORMATION PURSUANT TO A 2703(d) ORDER	6
CONCLUSION	7
CERTIFICATE OF SERVICE	
CERTIFICATE OF COMPLIANCE	

TABLE OF CITATIONS

Federal Cases E	Pages
Abdelfattah v. U.S. Dept. of Homeland Sec., 488 F.3d 178 (3d Cir. 2007)	34
Buczek v. Cont'l Cas. Ins. Co., 378 F.3d 284 (3d Cir. 2004)	33
Garcia v. United States, 469 U.S. 70 (1984)	18
In re Application, 2007 WL 3036849 (S.D. Tex. Oct. 17, 2007)	12
In re Applications, 509 F. Supp. 2d 76 (D. Mass. 2007) ("Stearns D. Mass. Opinion")	7, 19
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)	22
In re United States Application for an Order Authorizing Installation and Use of a Pen Register, 415 F. Supp. 2d 211 (W.D.N.Y. 2006)	15
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)	
In re Application of United States for an Order for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) ("Gorenstein S.D.N.Y. Opinion") 9, 1	9, 31
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)	. 15
In re Indian Palms Assoc., Ltd., 61 F.3d 197 (3d Cir. 1995)	34
In the Matter of the Application of the United States, etc.,534 F.Supp. 2d 585 (W.D. Pa. 2008)	5
Lame v. U.S. Dept. of Justice, 767 F.2d 66 (3d Cir. 1985)	34

Malloy v. Eichler, 860 F.2d 1179 (3d Cir. 1988)	18
Parastino v. Conestoga Tel & Tel. Co., No. Civ. A 99-679, 1999 WL 636664 (E.D. Pa. Aug. 18, 1999)	36
Rosenberg v. XM Ventures, 274 F.3d 137 (3d Cir. 2001)	23
SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984)	
Smith v. Maryland, 442 U.S. 735 (1979)	7, 28
Staples v. United States, 511 U.S. 600 (1994)	9
Tavarez v. Klingensmith, 372 F.3d 188 (3d Cir. 2004)	24
United States v. Bennett, 100 F.3d 1105 (3d Cir. 1996)	2
United States v. Gbemisola, 225 F.3d 753 (D.C. Cir. 2000)	
United States v. Grape, 549 F.3d 591 (3d Cir. 2008)	34
United States v. Introcaso, 506 F.3d 260 (3d Cir. 2007)	9
United States v. Jones, 471 F.3d 478 (3d Cir. 2006)	9
United States v. Karo, 468 U.S. 705 (1984)	ssim
United States v. Knotts, 460 U.S. 276 (1983)	9, 29
United States v. Kington, 801 F.2d 733 (5th Cir. 1986)	36
United States v. Miller, 425 U.S. 435 (1976)	. 26
United States v. Schneider, 14 F.3d 876 (3d Cir. 1994)	22
United States v. Thornton, 306 F.3d 1355 (3d Cir. 2002)	14

United States v. Weaver, 267 F.3d 231, 235 (3d Cir. 2001)	2
United States v. Willaman, 437 F.3d 354 (3d Cir. 2006)	33
Victaulic Co. v. Tieman, 499 F.3d 227 (3d Cir. 2007)	32
<u>Federal Statutes</u>	<u>Pages</u>
18 U.S.C. § 2510	11
18 U.S.C. § 2510(1)	11. 17, 20
18 U.S.C. § 2510(8)	11
18 U.S.C. § 2510(12)	17, 21
18 U.S.C. § 2510(15)	10
18 U.S.C. § 2511(1)	21
18 U.S.C. § 2701	
18 U.S.C. § 2703	
18 U.S.C. § 2703(a)	
18 U.S.C. § 2703(b)	10
18 U.S.C. § 2703(c)	passim
18 U.S.C. § 2703(d)	passim
18 U.S.C. § 2711(1)	
18 U.S.C. § 3117	
18 U.S.C. § 3123(a)	
28 U.S.C. § 636	
28 U.S.C. §1291	
47 U.S.C. § 222(c)	
47 U.S.C. § 222(f)	
47 U.S.C. § 1002	

47 U.S.C. § 1002(a)
Electronic Communications Privacy Act ("ECPA") § 101, P.L. 99-508, 100 Stat. 1848 (1986)
Communications Assistance for Law Enforcement Act ("CALEA") Pub. L. 103-414 § 207(a) (1994)
<u>Federal Rules</u> <u>Pages</u>
Fed. R. Crim. P. 41
Fed. R. Crim. P. 59
Fed. R. Evid. 201(b)
Other Authorities Pages
In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 15 FCC Rcd. 17442 (Sept. 8, 2000)
In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 16 FCC Rcd. 18305 (Oct. 12, 2001)
In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 16 FCC Rcd. 18305 (Oct. 12, 2001)
In re Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, 16 FCC Rcd. 18305 (Oct. 12, 2001)

No.08-4227

IN THE UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

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

Appeal from Memorandum Order Entered by the United States District Court for the Western District of Pennsylvania (McVerry, J.) at Magistrate No. 07-524M

BRIEF FOR THE UNITED STATES

JURISDICTION

This is a direct appeal stemming from the decision and Order of the district court denying an appeal by the government from a magistrate judge's order. The district court had jurisdiction over the appeal pursuant to Fed. R. Crim. P. 59 and 28 U.S.C. § 636. The United States filed a timely notice of appeal on October 10, 2008 (App. 1; App. 62, Docket No. 33).¹

This Court has jurisdiction to decide the appeal pursuant to 28 U.S.C. §1291.

1

¹ All record citations refer to the appendix filed by the appellant.

ISSUES PRESENTED and STANDARDS OF REVIEW

- 1. Whether the district court erred in holding that the government is barred as a matter of law from obtaining, pursuant to 18 U.S.C. § 2703(d), historical cell-site location information concerning a wireless telephone subscriber's usage of a cellular phone.
 - (a) This issue was preserved (App. 63-1).
- (b) The standard of review for this Court is "plenary review over the district court's determination of questions of law." <u>United States v. Bennett</u>, 100 F.3d 1105, 1107 n.1 (3d Cir. 1996).
- 2. Whether the district court erred as a matter of law in holding, without any evidentiary record before it, that the Fourth Amendment requires the government to seek a warrant based on probable cause in order to compel a wireless telephone carrier to disclose routine business records reflecting a subscriber's historical cell-site usage.
 - (a) This issue was preserved (App. 63-1).
- (b) The standard of review for this Court on questions of law is plenary review. <u>Bennett</u>, 100 F.3d at 1107 n.1. The standard of review on questions of fact is clear error. <u>United States v. Weaver</u>, 267 F.3d 231, 235 (3d Cir. 2001), <u>cert. denied</u>, 122 S. Ct. 1118 (2002).

STATEMENT OF RELATED PROCEEDINGS

This case has not been before this Court previously. Counsel is not aware of any related case or proceeding -- completed, pending, or anticipated -- before this Court or any other court or agency, state or federal.

STATEMENT OF THE CASE

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 under 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 November 21, 2007, the United States submitted an application at Magistrate's No. 07-524M with Magistrate Judge Lisa Pupo Lenihan of the Western District of Pennsylvania seeking a 2703(d) order directing a wireless telephone provider to disclose routine business records reflecting historical connection and cell-site information² associated with a specified cell phone (App. 64-68).³ The Application stated that the requested cell phone records are relevant and material to an ongoing investigation into large-scale narcotics trafficking and various related violent crimes.

² Historical cell site information includes only the service provider's record of prior usage of a cell phone and does not include any information concerning the content of any communications.

³ The Appendix contains the redacted version of the Application made available to amici by the District Court. The original non-redacted Application is available to this Court separately for in camera review through the district court clerk's office. The application was not docketed by the magistrate judge in the district court until February 22, 2008 (App. 59, Docket No. 2).

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 Application sought historical (but not prospective) cell-site records concerning a phone known to be used by the subject.

On February 19, 2008, without requesting briefing on the underlying legal and factual issues, 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 (App. 5-56).⁴ On March 3, 2008, the United States timely lodged its Objections and Notice of Appeal to the District Court (App. 63-1). On September 10, 2008, District Court Judge Terrence F. McVerry, while noting the importance and complexity of the matter and the lack of precedent in the Third Circuit, summarily affirmed the denial of the Application without hearing oral argument (App. 2-3). The government filed a Notice of Appeal on October 10, 2008 (App. 1; App. 62, Docket No. 33, Notice of Appeal).

⁴ The Opinion was joined by the other four full-time magistrate judges of the district (App. 56). The Magistrate Judge's Opinion and Order was docketed on February 22, 2008 (App. 59, Docket No. 3). The Magistrate Judge's Opinion is reported. In the Matter of the Application of the United States, etc., 534 F.Supp. 2d 585 (W.D. Pa. 2008).

As of the date of the filing of this brief, the investigation in question remains active and ongoing and the information which is sought by the government through its Application has not been obtained.

SUMMARY OF ARGUMENT

Section 2703(d) permits the government to obtain a court order compelling the disclosure of 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, a request for historical cell-site information based upon specific and articulable facts establishing reasonable grounds satisfies each of the requirements of the statute, a position endorsed in recent months by several other courts.

In reaching the opposite conclusion, the Opinion and Order⁵ contains, and relies upon, numerous errors, both as to the facts of the underlying technology and as to the interpretation of applicable law. Indeed, as discussed below, 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, the government respectfully urges the Court to reverse and remand with instructions to grant the Application.

⁵ Because the district court summarily affirmed without further legal analysis, this brief will directly address the legal errors in the magistrate judge's written opinion.

ARGUMENT

I. THE GOVERNMENT MAY COMPEL A WIRELESS SERVICE PROVIDER TO DISCLOSE HISTORICAL CELL-SITE RECORDS PERTAINING TO A SUBSCRIBER BY MEANS OF A COURT ORDER ISSUED UNDER 18 U.S.C. § 2703(d).

Cellular telephone companies keep, in the regular course of their business, records of certain information associated with their customers' calls. As reflected in the exemplar submitted to the district court⁶ (App. 63), 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.⁷ No such record is created when the phone is not in use.

The exemplar is from the same wireless carrier from which the government seeks to obtain records in this proceeding. Because these records contain sensitive information pertaining to a prior investigation, certain identifying information—the telephone numbers involved—has been redacted.

The first line of the exemplar 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 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.

⁷ 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 only identifies which of the three 120°, pie-slice sectors where the phone was probably located.

Although historical cell tower records provide limited information, that information is useful to law enforcement because it provides a general indication of where a cell phone call was made. As one court has explained,

[t]he 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) ("Gorenstein S.D.N.Y. Opinion") (citation omitted). No Global Positioning System ("GPS") data or other more precise location information (such as "triangulation" data) is contained in the historical records requested pursuant to the Application. Indeed, cell-site records do not even indicate a phone's distance from the serving tower, let alone its specific location.

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

As this Court has often reiterated, "[t]he plain language of the statute is the starting place in our inquiry." <u>United States v. Introcaso</u>, 506 F.3d 260, 264 (3d Cir. 2007) (<u>quoting Staples v. United States</u>, 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." <u>Id.</u> (<u>quoting United States v. Jones</u>, 471 F.3d 478, 480 (3d Cir. 2006)).

⁸ In order to attempt to avoid any confusion, the government will, in making references in its second and subsequent citations to other reported district court opinions involving government applications under §2703(d) (which also read "In re Application ... ", etc.), identify the case by use of the name of the authoring district court judge and the judicial district.

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. See 18 U.S.C. § 2703(c)(1). As explained below, cell-site information 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) and 2711(1). Cell phone service providers provide their customers with the ability to send "wire

⁹ 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 relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

communications,"¹⁰ and thus they are providers of electronic communication service.

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 Gorenstein S.D.N.Y. Opinion, 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 had 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 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

¹⁰ A "wire communication" necessarily involves the human voice. <u>See</u> § 2510(1) (defining "wire communication") and § 2510 (defining "aural transfer"); S. Rep. No. 541, 99th Cong., 2d Sess. 11 (1986), <u>reprinted in</u> 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").

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, Pub. L. No. 99-508, 100 Stat. 1848, 1862 (1986). The accompanying 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. 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).

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, United States District Court Judge Rosenthal in Houston confronted a similar situation: a magistrate judge had denied the government's application for, <u>inter alia</u>, historical cell-site data under the authority of § 2703(d). <u>See In re Application</u>, 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.

B. No Other Statutory 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 focuses on determining the proper authority for obtaining such information **prospectively**. Prospective cell-site information, however, is not at issue in this case. The decision never fully recovers from this erroneous presumption, and as a result conflates the legal principles actually relevant to the government's Application.

In the course of the analysis, the Magistrate Judge relies upon several statutes as purportedly limiting 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 at 18 U.S.C. § 3117; and the text of § 2703 itself all bar the government from compelling disclosure of historical 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 of Title 18 is likewise inapplicable because a user's own phone is not a "tracking device" within the narrow meaning of that statute. However, § 2703 not only applies, but on its

face § 2703, which the government invoked in its Application, expressly permits the government's current Application. None of these authorities prohibits, or even limits in any way, the compelled production of historical cell-site information authorized pursuant to a 2703(d) order. 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 significant discussion to 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. To 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." <u>United States v. Thornton</u>, 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. No. 103-414, § 207(a) (1994).¹¹

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.¹²

The Magistrate Judge's opinion acknowledges the prior decisions holding (or implying) that historical cell-site records may be obtained by way

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" showing "reasonable grounds" 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.

Magistrates and district courts in several districts 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 (App. 30), 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."); In re United States Application for an Order Authorizing Installation and Use of a Pen Register, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) ("the SCA authorizes the government to obtain historical cell-site data, including location information") (emphasis in original).

of § 2703(d). Simultaneously, however, the decision below dismisses that same precedent with the unsupported claim that the legal distinction between prospective and historical cell-site records is "largely-unexplained." (App. 34). In fact, the government submits that the distinction between the two 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 incorrectly disregards this fundamental dichotomy. Because the Opinion and Order improperly relies on the CALEA limitation (and cases applying it to prospective surveillance) to conclude that the statutes "do not distinguish between historic[al] and prospective [cell-site records]" (App. 6), its flawed analysis should be rejected.

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

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 (App. 32-41). That conclusion, however, is unsound. 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 scope 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." 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, correctly analyzed under the statute, historical cell-site information concerning a wireless telephone call is plainly "a record or other information pertaining to a subscriber" who uses a service provider's network to send and receive "wire communications." See Stearns D. Mass. Opinion, 509 F. Supp. 2d at 80 (reversing magistrate judge's contrary conclusion).

The essential distinction is that a "wire communication" necessarily involves the human voice. See § 2510(1) (defining "wire communication") and § 2510 (defining "aural transfer").

The decision below overlooks these clearly articulated distinctions. Instead, the Opinion focuses on the definition of an inapposite term ("electronic communication"). Having done so, the Opinion and Order further distorts the statute by construing the straightforward 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).

(App. 37) (emphasis in original) (footnote omitted). Because this 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 erred in finding that the target cell phone is 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 empower a court to authorize out-of-district 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."); Gorenstein S.D.N.Y. Opinion, 405 F. Supp. 2d 435, 449 n.8 (S.D.N.Y. 2005) (same).

The legislative history of § 3117, enacted as part of ECPA,¹⁴ is equally clear that "tracking devices" are homing devices, not cell phones or other communications technologies. Most obviously, the 1986 House Report cites the two landmark Supreme Court decisions concerning "beeper" homing devices, <u>United States v. Knotts</u>, 460 U.S. 276 (1983) (beeper installed in can of chloroform and used to track movements of car) and <u>United States v. Karo</u>, 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

¹⁴ See Pub. L. No. 99-508, 100 Stat. 1848, § 108 (1986).

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), <u>reprinted in</u> 1986 U.S. Code Cong. & Admin. News 3555, 3564.

Even more revealing is the fact that the very same 1986 legislation 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. 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.

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 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 expressly intended them to have. If cell phones were classified as "tracking devices," text messages or e-mail transmitted from cell phones (which are not wire or oral communications) 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, at *2 (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. ¹⁵ For this reason as well, the decision below should be reversed.

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 (App. 41-44). This conclusion allegedly flows from the express language and structure of § 2703. On the contrary, the text of the statute allows no such 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.

The Opinion and Order asserts that the use of tracking devices pursuant to 18 U.S.C. § 3117 requires probable cause (App. 21). 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." <u>Id.</u> 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 section.") (emphasis in original); Gorenstein S.D.N.Y. Opinion, 405 F. Supp. 2d at 449 n.8 (same).

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).

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., Tavarez 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. No. 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. No. 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.

For all of the above reasons, an order under the standard set out at 18 U.S.C. § 2703(d) may be used to compel historical cell-site records, and the decision below denying the Application should therefore be reversed.

II. 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 (App. 46-55). This conclusion is incorrect for two distinct reasons. First, under the established principles of <u>United States v. Miller</u>, 425 U.S. 435 (1976), and <u>Smith v. Maryland</u>, 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.

A. A Subscriber Has No Expectation of Privacy in Historical Cell-site Records Held by a Third Party

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 <u>United States v. Miller</u>, 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." <u>Miller</u>, 425 U.S. at 440; <u>see also SEC v. Jerry T. O'Brien, Inc.</u>, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party ... he

Thus, but for 18 U.S.C. § 2703(d), the records at issue in this case could be compelled via subpoena.

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 usage information, that 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 and identity of the cell phone tower handling a customer's call is generated internally by the phone company and is not, therefore, 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.

Further, even if it were the case that cell-site information is disclosed by the subscriber to the telephone company, the Supreme 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. When a cell phone user transmits a signal to a cell tower for his call to be connected, he thereby assumes the risk that the cell phone provider will create its own internal record of which of its towers handles the call. 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.

B. 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 a business record in the possession of a third party, cell-site information should not be judged under Fourth Amendment standards applicable to 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 Karo, 468 U.S. at 713) (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).

At issue in <u>Karo</u> was 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." <u>Id.</u> 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. <u>Id.</u> 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. <u>See id.</u> 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." <u>Id.</u> 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. <u>Id.</u> 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.

<u>Id.</u> at 720 (emphasis added). In sum, the test under <u>Karo</u> 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. <u>See id.</u> n.6.) Rather, <u>Karo</u> 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.

1. The Lower Court's Factual Claim That Historical Cell-Site Information Can Locate a Phone "Within Approximately 200 Feet" Is Clearly Erroneous

In support of its conclusion that historical cell-site location information is subject to Fourth Amendment protections, the Opinion and Order's "Technological Development Overview" asserts that "the location of just the nearest tower itself can place the phone within approximately 200 feet" (App. 13). Because the record below contains no support whatsoever for this incorrect assertion, this Court should reject both the factual claim and the lower court's flawed legal conclusions based upon it.

In making this 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, <u>The Fourth Amendment and Cell Phone Location</u> <u>Tracking: Where Are We?</u>, 29 Hastings Comm. & Ent. L.J. 421, 426-27 (Spring 2007). In turn, that author's sole source for his claims is the <u>Gorenstein S.D.N.Y. Opinion</u>, 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).

As this Court has noted repeatedly, judicial notice may be taken only of facts not subject to reasonable dispute. See, e.g., Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007); see also Fed. R. Evid. 201(b). Thus, a judicially noticed fact must either be one generally known within the trial court's jurisdiction or "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Fed. R. Evid. 201(b). Even then, a district court should indulge in judicial notice only "sparingly" when it does so "outside the context of an evidentiary proceeding." Victaulic Co., 499 F.3d at 236.

The lower court's factual claim fails each and every one of these criteria, and accordingly should be rejected as clearly erroneous. To begin with, the Magistrate Judge did so without benefit of any evidentiary submissions or other briefing, formal or informal, written or oral. The Opinion below then compounded this error by relying on a single passage in a factually inaccurate law student note, 17 hardly a source "whose accuracy cannot reasonably be

The Opinion and Order relies on the same student note for the equally incorrect claim that a wireless phone can be tracked to within 50 feet using its GPS capability (App. 13). Aside from the fact that the student note does not make or support this assertion, this claim is in any event irrelevant to the government's Application. As noted explicitly in all of the FCC documents referenced below (Fn. 18), GPS-based and other **prospective** location-finding capabilities ("E911 Phase II") 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 Application seeks only historical cell-site

questioned." But most tellingly, the lone case upon which the student note relies for its claim of accuracy of "a couple hundred feet" – the <u>Gorenstein S.D.N.Y. Opinion</u> – **does not in fact support that proposition**.

Further, on appeal to the district court, the government vigorously disputed the Magistrate Judge's factual claim. The district court nevertheless summarily affirmed, notwithstanding the elementary proposition that a "disputed fact is not one that is appropriate for judicial notice." Buczek v. Cont'l Cas. Ins. Co., 378 F.3d 284, 291 (3d Cir. 2004); accord United States v. Willaman, 437 F.3d 354, 361 (3d Cir. 2006). In doing so, the district court disregarded the government's citation to multiple contrary 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). 18 The

⁻that is, tower and sector-records. It does not seek GPS or "triangulation" information. Rather, the government has requested only the type of records shown in the record exemplar provided to the court below (App. 63).

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).

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." <u>Id.</u>

Factual findings are clearly erroneous when they are "unsupported by substantial evidence, lack adequate evidentiary support in the record, are against the clear weight of the evidence or where the district court has misapprehended the weight of the evidence." Abdelfattah v. U.S. Dept. of Homeland Sec., 488 F.3d 178 (3d Cir. 2007) (quoting Lame v. U.S. Dept. of Justice, 767 F.2d 66, 70 (3d Cir. 1985)). Here, there is no evidence in the record to support the magistrate judge's factual finding that cell-site information is accurate to within 200 feet. Thus, the Magistrate Judge's finding is clearly erroneous. Accordingly, the lower court's claim that historical cell-site information is accurate "within approximately 200 feet" should be reversed as clearly erroneous.¹⁹

2. Even Assuming the Truth of the Lower Court's Unsupported "200 Foot Accuracy" Claim, No Fourth Amendment Interests Are Implicated

Even if this Court were to accept the disputed finding below that historical cell-site location information is accurate to within 200 feet, it should nevertheless reverse the lower court's holding that such information infringes a Fourth Amendment privacy interest. As discussed above, <u>Karo</u> holds that government use of a tracking device violates the Fourth Amendment only where the monitoring actually reveals the **particular** private location in which

Further, the government observes that it would be wholly proper for this Court itself to take judicial notice of the FCC factual findings noted above. See <u>In re Indian Palms Assoc., Ltd.</u>, 61 F.3d 197, 205-06 (3d Cir. 1995) ("Judicial notice may be taken at any stage of the proceeding, including on appeal"); <u>accord United States v. Grape</u>, 549 F.3d 591, 604 n.11 (3d Cir. 2008).

the tracked object may be found. The Supreme Court expressly held that no search occurred in <u>Karo</u> even when law enforcement tracked the can of ether in real time to a given storage facility or even a specific row of lockers, but not to a specific storage locker. <u>See</u> 468 U.S. at 720.

With a purported 200-foot margin of error, cellular phone companies' historical records of cell-site usage are therefore 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 Gorenstein S.D.N.Y. Opinion, 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 result, this Court should reverse and find that the Fourth Amendment poses no obstacle to the use of 2703(d) order to compel historical cell-site information from a wireless carrier.

C. Federal Statutory Law Does Not Confer Additional Fourth Amendment Rights

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." (App. 27).

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.

<u>United States v. Kington</u>, 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.

CONCLUSION

For the foregoing reasons, the order of the district court denying the Application should be reversed and this case remanded with instructions to grant the Application.

Respectfully submitted,

MARY BETH BUCHANAN United States Attorney

/s/Robert L. Eberhardt Robert L. Eberhardt Assistant United States Attorney

CERTIFICATE OF COMPLIANCE

- 1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains **9,898** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).
- 2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportional typeface using WordPerfect 12 in Times New Roman 14 point font.
 - 3. The text of this e-brief and hard copies of the brief are identical.
- 4. A virus check was performed on both this e-mail and e-brief with Trend Micro OfficeScan Version 6.5.

/s/Robert L. Eberhardt Robert L. Eberhardt Assistant U.S. Attorney

CERTIFICATE OF SERVICE

I hereby certify that the following are filing users and will be served electronically by the Notice of Docketing Activity. Two copies of this brief were also sent by First Class Mail to:

Witold J. Walczak, Esq. Email: www.www.aclupa.org American Civil Liberties Union 313 Atwood Street Pittsburgh, PA 15213-0000

Lisa B. Freeland, Esq. Email: <u>Lisa Freeland@fd.org</u> Federal Public Defender 1450 Liberty Center 1001 Liberty Avenue Pittsburgh, PA 15222:

> /s/Robert L. Eberhardt Robert L. Eberhardt Assistant U.S. Attorney

Dated: February 13, 2009