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 U.S. District Court for the Western District of Pennsylvania (McVerry, J.) at Magistrate No. 07-524M

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, THE AMERICAN CIVIL LIBERTIES UNION, THE ACLU-FOUNDATION OF PENNSYLVANIA, INC., AND THE CENTER FOR DEMOCRACY AND TECHNOLOGY IN SUPPORT OF AFFIRMANCE OF THE DISTRICT COURT

Respectfully submitted,

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Attorneys for *Amici Curiae*

On the brief:

Jennifer Granick
Kevin Bankston
Matthew Zimmerman
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
jennifer@eff.org
bankston@eff.org
mattz@eff.org

Jim Dempsey
Harley Geiger
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
202-637-9800
jdempsey@cdt.org
harley@cdt.org

Catherine Crump
American Civil Liberties Union Found.
125 Broad Street, 18th Floor
New York, NY 10004
212-519-7806
ccrump@aclu.org

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 U.S. District Court for the Western District of Pennsylvania (McVerry, J.) at Magistrate No. 07-524M

BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION, THE AMERICAN CIVIL LIBERTIES UNION, THE ACLU-FOUNDATION OF PENNSYLVANIA, INC., AND THE CENTER FOR DEMOCRACY AND TECHNOLOGY IN SUPPORT OF AFFIRMANCE OF THE DISTRICT COURT

Respectfully submitted,

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Attorneys for *Amici Curiae*

On the brief:

Jennifer Granick
Kevin Bankston
Matthew Zimmerman
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333
jennifer@eff.org
bankston@eff.org
mattz@eff.org

Jim Dempsey
Harley Geiger
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006
202-637-9800
jdempsey@cdt.org
harley@cdt.org

Catherine Crump
American Civil Liberties Union Found.
125 Broad Street, 18th Floor
New York, NY 10004
212-519-7806
ccrump@aclu.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES iv

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION vi

STATEMENT OF AMICI CURIAE vii

INTRODUCTION AND SUMMARY OF ARGUMENT 1

ARGUMENT

I. The Stored Communications Act Requires the Government to Obtain at Least an Order Under 18 U.S.C. § 2703(d) Before Obtaining CSLI. 2

II. The SCA Gives the Court the Discretion to Deny an Application for an Order Under 18 U.S.C. § 2703(d) and Instead Require the Government to Seek a Probable Cause Warrant. 3

A. The Plain Language of 18 U.S.C. § 2703(d) is Permissive and Does Not Require Issuance of an Order Upon a Showing of Specific and Articulable Facts. 4

B. The Permissive Reading of 18 U.S.C. § 2703(d) is Required By Rather Than Foreclosed By the Rule Against Superfluities. 4

C. The Permissive Reading of 18 U.S.C. § 2703(d) is Supported By Rather Than Contradicted By Legislative History. 7

D. This Court is Required By the Doctrine of Constitutional Avoidance to Adopt the Permissive Reading of 18 U.S.C. § 2703(d). 9

1. The Constitutional Avoidance Doctrine Requires This Court to Adopt the Plausible Reading of the SCA That Will Avoid Serious Constitutional Questions. 9

2. The Mandatory Reading of 18 U.S.C. § 2703(d) Raises Serious Constitutional Questions About the Constitutionality of the SCA. 10

III. The Fourth Amendment Requires That the Government Seek a Warrant to Obtain CSLI. 13

A. CSLI Can Be and Routinely Is Used By the Government to Locate Individuals and Their Cell Phones Within Private Spaces. 14

B. A Cell Phone User Does Not Knowingly Expose Her Phone's Location Whenever She Turns It On or Uses It. 19

IV. If the Court Believes That the Accuracy of the CSLI at Issue is Relevant, It Must Remand for an Evidentiary Hearing. 22

CONCLUSION 23

CERTIFICATE OF COMPLIANCE 24

CERTIFICATE OF SERVICE 25

TABLE OF AUTHORITIES

Federal Cases **Pages**

Almendarez-Torres v. United States, 523 U.S. 224 (1998) 10

Bond v. United States, 529 U.S. 334 (2000) 13

California v. Hodari D., 499 U.S. 621 (1991) 4

California Bankers Assn. v. Shultz, 416 U.S. 21 (1974) 20

Clark v. Martinez, 543 U.S. 371 (2005)..... 9, 11

Duncan v. Walker, 533 U.S. 167 (2001)..... 6

In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005)..... 11, 21

In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 846 F. Supp. 1555 (M.D. Fla. 1994)..... 5

In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585 (W.D. Pa. 2008)..... *passim*

Kyllo v. United States, 533 U.S. 27 (2001)..... 17, 18, 19, 22

Miller-El v. Cockrell, 537 U.S. 322 (2003)..... 4

Rosenberg v. XM Ventures, 274 F.3d 137 (3rd Cir. 2001) 2

Smith v. Maryland, 442 U.S. 735 (1979) 19, 20, 21, 22

Tavarez v. Klingensmith, 372 F.3d 188 (3rd Cir. 2004)..... 5

United States v. Berry, 300 F. Supp. 2d 366 (D. Md. 2004)..... 19

United States v. Forest, 355 F.3d 942 (6th Cir. 2004) 21

United States v. Fregoso, 60 F.3d 1314 (8th Cir. 1995)..... 5

United States v. Garcia, 474 F.3d 994 (7th Cir. 2007)..... 13

United States v. Karo, 468 U.S. 705 (1984)..... *passim*

United States v. Knotts, 460 U.S. 276 (1983) 13, 14, 17

United States v. Miller, 425 U.S. 435 (1976)..... 19, 20, 22

United States v. Oakland Cannabis Buyers' Coop., 532 U.S. 483 (2001)..... 9

United States v. X-Citement Videos, Inc., 513 U.S. 64 (1994) 9

United States ex rel. Attorney General v. Delaware & Hudson Co., 213 U.S. 366 (1909) 9

Federal Statutes **Pages**

18 U.S.C. § 2703(d) ..... *passim*

18 U.S.C. § 2703(c) ..... *passim*

18 U.S.C. § 3123(a) 5

18 U.S.C. § 2510(15). 20

Federal Rules **Pages**

Fed R. Crim. P. 41 ..... 3, 6

Fed. R. App. P. 26.1 iii

Fed. R. App. P 32(a) 21

Fed. R. App. P. 25(a) 22

Other Authorities **Pages**

S. Rep. No. 99-541 (1986) 7

S. Hrg. 98-1266 (1984) 7

H.R. Rep. No. 99-647 (1986) 7, 8

H.R. Rep. No. 103-827 (1994) 7, 8

47 C.F.R. § 20.18(h)(1) (2008) 12

CTIA-THE WIRELESS ASSOCIATION, MID-YEAR 2008 TOP-LINE SURVEY RESULTS (2008) 12, 23

Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators, 18 Harv. J. L. & Tech. 307 (Fall 2004) 12

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Federal Rule of Appellate Procedure 26.1, *Amici* Electronic Frontier Foundation ("EFF"), ACLU-Foundation of Pennsylvania, Inc. ("ACLU of Pennsylvania"), American Civil Liberties Union, and Center for Democracy and Technology ("CDT"), non-profit corporations, make the following disclosure:

1. No *Amicus* is a publicly held corporation or other publicly held entity.

2. *Amici* have no parent corporations.

3. No publicly held corporation or other publicly held entity owns 10% or more of any *Amicus*.

4. No *Amicus* is a trade association.

DATED: March 16, 2009

By Witold Walczak

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Attorneys for *Amici Curiae*

STATEMENT OF AMICI CURIAE

Amici are non-profit public interest organizations seeking to ensure the preservation of Fourth Amendment and statutory privacy protections in the face of advancing technology. This *amicus* brief is submitted at the request and by the order of this Court, under its Briefing Order dated January 26, 2009.

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported civil liberties organization working to protect free speech and privacy rights in the online world. As part of that mission, EFF has served as counsel or *amicus* in key cases addressing electronic privacy statutes and the Fourth Amendment as applied to the Internet and other new technologies. With more than 10,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of liberty and equality embodied in the U.S. Constitution. The protection of privacy as guaranteed by the Fourth Amendment is an area of special concern to the ACLU. In this connection, the ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy in Internet communications.

The ACLU-Foundation of Pennsylvania, Inc. ("ACLU of Pennsylvania") is a non-profit organization with about 19,000 members in Pennsylvania. The organization is devoted to the preservation and

advancement of civil liberties for all Pennsylvanians through public education, legislative advocacy and litigation. The ACLU of Pennsylvania regularly appears in this Court and the Third Circuit as either direct counsel or amicus to serve those ends. Because of its particular commitment to rights of privacy and due process, the ACLU of Pennsylvania has a special interest in, and expertise to address, the application of the law in this case.

The Center for Democracy and Technology ("CDT") is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet and other communications networks. CDT represents the public's interest in an open, decentralized Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

INTRODUCTION AND SUMMARY OF ARGUMENT

Amici urge this court to affirm the District Court's decision upholding the Magistrate Judge's denial of the Government's application under 18 U.S.C. § 2703(d) to obtain cell site location information ("CSLI"). *See* McVerry Order of September 10, 2008 (Government Appendix ("Gov. App.") 2, Docket No. 31), *aff'g In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) (Gov. App. 5, Docket No. 3) ("M.J. Order").

Amici agree with the Government that the Stored Communications Act ("SCA") protects CSLI, establishing a statutory floor of privacy protection by requiring the Government to obtain at least an order under 18 U.S.C. § 2703(d) (a "D Order") before compelling its disclosure from a cell phone provider. However, the Magistrate Judge was correct that the SCA permits but does not require her to issue an order under that section, a holding required by the statute's plain language and the canons of construction. By giving judges the discretion to deny an application for a D Order and instead require the Government to obtain a search warrant under the Federal Rules of Criminal Procedure pursuant to 18 U.S.C. § 2703(c)(1)(a), Congress set a sliding scale for access to information covered by the SCA and thus provided a statutory "safety-valve" to judges faced with requests for information that is or may be protected by the Fourth Amendment, allowing them to avoid issuing an order that may violate the Fourth Amendment or call the statute's constitutionality into question.

Even assuming that the statutory language in question is ambiguous and subject to more than one fair reading, *Amici* need only show that the

Government's "mandatory" reading of 18 U.S.C. § 2703(d) raises serious constitutional questions in order for the doctrine of constitutional avoidance to require the Magistrate Judge's "permissive" reading. However, *Amici* also demonstrate that CSLI, which reveals information about the interior of protected spaces such as the home, is in fact protected by the Fourth Amendment. *Amici* further demonstrate how the accuracy of CSLI is irrelevant to this analysis and urges the Court to remand for an evidentiary hearing if it determines otherwise.

ARGUMENT

I. The Stored Communications Act Requires the Government to Obtain at Least an Order Under 18 U.S.C. § 2703(d) Before Obtaining CSLI.

"[E]very exercise of statutory interpretation begins with an examination of the plain language of the statute," and where statutory language is "plain and unambiguous," no further inquiry is necessary. *Rosenberg v. XM Ventures,* 274 F.3d 137, 141 (3rd Cir. 2001). *Amici* agree with the Government that the Stored Communications Act portion of the Electronic Communications Privacy Act ("ECPA") plainly and unambiguously protects stored CSLI as "a record or other information pertaining to a subscriber to or customer of [an electronic communication] service." 18 U.S.C. § 2703(c)(1); *see also* Government's Appellate Brief of February 13, 2009 ("Gov. Br."), at 9-13.[1]

Magistrate Judge Lenihan was correct to find that Congress,

[1] *Amici* further agree with the Government that CSLI constitutes such "a record or other information" regardless of whether a cell phone is a "tracking device." *See* Gov. Br. at 16-18. Because the question of whether a cell phone may be a "tracking device" is irrelevant, *Amici* do not take a position on it, and do not adopt the Government's additional argument that a cell phone can never be a "tracking device." Gov. Br. 18-23.

"recogniz[ing] the importance of an individual's expectation of privacy in her physical location," intended to protect the privacy of CSLI against governmental intrusion. M.J. Order, 534 F. Supp. 2d at 610. However, it is *through the SCA* that Congress provided such protection. The SCA provides a clear statutory floor of protection for such information, requiring that the government obtain *at least* a court order issued under 18 U.S.C. § 2703(d) before obtaining such information. *See* 18 U.S.C. § 2703(c)(1)(B).

II. The SCA Gives the Court the Discretion to Deny an Application for an Order Under 18 U.S.C. § 2703(d) and Instead Require the Government to Seek a Probable Cause Warrant.

While the SCA recognizes that some information pertaining to a subscriber should be available with a mere subpoena, and while it provided at least the protection of a D Order for other non-content, the statute also expressly recognizes that some of this information may require a warrant. *See* 18 U.S.C. § 2703(c)(1)(A). Accordingly, as Magistrate Judge Lenihan correctly held that 18 U.S.C. § 2703(d) gives courts the discretion to deny an application for a D Order even when the specific and articulable facts standard has been met and thereby require the government to instead seek a warrant under Rule 41 of the Federal Rules of Criminal Procedure pursuant to 18 U.S.C. § 2703(c)(1)(a). M.J. Order, 534 F. Supp. 2d at 607-09. This "permissive" reading of § 2703(d) is required by the statute's plain language, the rule against superfluities, and Congress' intent to provide courts with a statutory "safety-valve" to avoid issuing orders that may violate the Fourth Amendment. Indeed, this reading is required by the doctrine of constitutional avoidance that instructs magistrate judges — and this Court — to avoid difficult Fourth Amendment questions.

A. The Plain Language of 18 U.S.C. § 2703(d) is Permissive and Does Not Require Issuance of an Order Upon a Showing of Specific and Articulable Facts.

The plain language of the Stored Communications Act supports Magistrate Judge Lenihan's conclusion that 18 U.S.C. § 2703(d) permits but does not require the Court to issue a D Order whenever the Government makes a showing of specific and articulable facts. Section 2703(d) reads:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue *only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the 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) (emphasis added). As the Magistrate Judge correctly held below:

> [Section 2703(d)] does not provide that such an Order shall issue 'if' or 'whenever' such a showing is made. Thus, under the plain language of the SCA, a showing of reasonable relevance is a *necessary*, but not necessarily *sufficient*, condition for issuance of an Order.

M.J. Order, 534 F. Supp. 2d at 608 (emphasis in original). *See also, e.g., California v. Hodari D.*, 499 U.S. 621, 628 (1991) ("'only if' . . . states a *necessary*, but not a *sufficient*, condition . . . .") (emphasis in original); *accord Miller-El v. Cockrell*, 537 U.S. 322, 349 (2003). By choosing the phrase "only if" rather than simply "if" in section 2703(d), Congress made clear that a court *may* issue but is not *required* to issue a D Order when the Government has made its specific and articulable facts showing.

B. The Permissive Reading of 18 U.S.C. § 2703(d) is Required By Rather Than Foreclosed By the Rule Against Superfluities.

The Government's proposed "mandatory" reading of 18 U.S.C. § 2703(d) — that a specific and articulable facts showing is always sufficient

to require the issuance of a D Order — would render Congress' use of the word "only" in that provision superfluous, as compared to Congress' language elsewhere in ECPA where it has provided for mandatory issuance of court orders based on a particular showing. *See Tavarez v. Klingensmith*, 372 F.3d 188, 190 (3rd Cir. 2004) (courts "must look to the surrounding words and provisions and their context," and give effect to every provision of a statute whenever possible).

In particular, Title II of ECPA, the Pen Register Statute ("PRS") governing the installation of "pen register" and "trap and trace devices" that capture non-content communications routing information, sets forth a mandatory standard under which courts *must* grant government applications for orders authorizing such surveillance:

> Upon an application made under section 3122(a)(1), the court *shall* enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, *if* the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

18 U.S.C. § 3123(a)(1) (emphasis added). Multiple courts have read the PRS' "shall...if" language to require issuance of a court order authorizing pen register or trap and trace surveillance where the government has made the appropriate certification, allowing the court little or no discretion. *See, e.g., United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995); *In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994)). In other words, courts have construed the PRS'

"shall...if" language to mean that the appropriate certification is a *sufficient* condition for the issuance of a surveillance order under the PRS.

The PRS' "shall...if" language stands in sharp contrast to the permissive "shall...only if" language found in 18 U.S.C. § 2703(d), language that Congress passed as part of the very same piece of legislation. If possible, the Court must "'give effect . . . to every clause and word of a statute.'" *See Duncan v. Walker*, 533 U.S. 167, 174 (2001) (citation omitted). For the "only" in 18 U.S.C. § 2703(d) to have any meaning, it must mean that a specific and articulable facts showing is a necessary but not necessarily sufficient condition for the issuance of a D Order. *See* M.J. Order, 534 F. Supp. 2d at 607-09.

The Government has offered no other plausible reading for the inclusion of a warrant standard in the sliding scale of authorities set forth in § 2703(c) or that gives the word "only" any effect and avoids the rule against superfluities. Instead, the Government misconstrues the Magistrate Judge's ruling to claim that it is she who violated the rule against superfluities: "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 render part of the statute superfluous." Gov. Br. at 24. However, the Magistrate Judge did not insist that § 2703(d) applications must set forth probable cause. Rather, she correctly held that § 2703(d) allows a court in individual cases to deny an application even when that showing has been made and thereby require the Government to instead pursue a warrant under Federal Rule of Criminal Procedure 41. *See* M.J. Order, 534 F. Supp. 2d at 616. This reading, rather than making section 2703(d) superfluous to section 2703(c)(1)(a)'s provision for warrants,

plainly *relies* on it. Indeed, it is the mandatory reading of section 2703(d) that renders section 2703(c)(1)(a) superfluous: there would never be any reason for the government to seek a warrant under that provision if it could in every case instead obtain a D Order under section 2703(d)'s more lenient standard.

C. The Permissive Reading of 18 U.S.C. § 2703(d) is Supported By Rather Than Contradicted By Legislative History.

Giving courts the flexibility to deny D Order applications and instead require warrants is consistent with the SCA's broad privacy-protective purpose which was based on Congress' recognition that as technology advanced, electronic communication service providers ("ECSPs") would progressively store more (and more invasive) types of records and other information with uncertain protection under the Fourth Amendment. As the Senate Judiciary Committee's report on ECPA explained:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.

S. Rep. No. 99-541 at 3 (1986); *see also, e.g.,* S. Hrg. 98-1266 at 17 (1984) ("In this rapidly developing area of communications which range from cellular non-wire telephone connections to microwave-fed computer terminals, distinctions such as [whether a participant to an electronic communication can claim a reasonable expectation of privacy] *are not always clear or obvious*.") (emphasis added).

Congress recognized that "in the face of increasingly powerful and personally revealing technologies," the requirement of a mere subpoena was not sufficient to protect the privacy of the increasing quantity and quality of

more invasive types of records threatening to reveal a "person's entire on-line profile." H.R. Rep. No. 103-827 at 13, 17 (1994). It therefore prohibited the Government from obtaining such records without at least a specific and articulable facts showing under 18 U.S.C. § 2703(d). *See* 18 U.S.C. § 2703(c)(1)(B). However, Congress also provided to courts a statutory safety-valve to ensure that privacy could always be adequately protected despite advances in technology. Through it's use of the word "only" in section 2703(d), Congress future-proofed the statute by permitting magistrates in their discretion to deny a D Order application and instead require a probable cause showing before authorizing the disclosure of particularly novel or invasive types of information that may be protected by the Fourth Amendment. In doing so, Congress gave courts the power to ensure that the SCA's allowance for D Orders would never violate the Fourth Amendment.[2]

[2] The legislative history that the Government cites does not call this conclusion into question. First, the government points to Congress' statement that "if a court order is sought then the government must meet the procedural requirements of subsection (d)." Gov. Br. at 24, quoting H.R. Rep. No. 99-647 (1986). Yet this statement only indicates that a specific and articulable facts showing is a necessary condition for the issuance of a D Order, not that such a showing is necessarily a sufficient condition. Second, the Government cites legislative indicating that the D Order standard is an "an intermediate standard . . . higher than a subpoena, but not a probable cause warrant." *Id.* at 25, quoting H.R. Rep. No. 103-827 (1994). Yet that statement misses the point: *Amici*'s disagreement with the Government is not over the meaning of "specific and articulable facts," but over the meaning of the phrase "only if."

D. This Court is Required By the Doctrine of Constitutional Avoidance to Adopt the Permissive Reading of 18 U.S.C. § 2703(d).

As demonstrated in the last section, Congress was well aware that the Fourth Amendment status of some records available to the government under 18 U.S.C. § 2703(c)(1) would be uncertain and would grow more uncertain as new and more invasive types of records emerged. Under the doctrine of constitutional avoidance, this Court cannot ascribe to Congress an intent that those records that are protected by the Fourth Amendment — such as CSLI, *see infra* at Section III — be obtainable under the SCA without a warrant. Instead, it must adopt the permissive reading of section 2703(d)'s "only if" language and affirm the Magistrate Judge's decision to instead require a warrant.

1. The Constitutional Avoidance Doctrine Requires This Court to Adopt the Plausible Reading of the SCA That Will Avoid Serious Constitutional Questions.

The constitutional avoidance doctrine "rest[s] on the reasonable presumption that Congress did not intend" any meaning of a statute "which raises serious constitutional doubts," *Clark v. Martinez*, 543 U.S. 371, 381 (2005), and "[i]t is therefore incumbent upon [the Court] to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress." *United States v. X-Citement Videos, Inc.*, 513 U.S. 64, 78 (1994); *see also Clark*, 543 U.S. at 384 (courts must adopt any "plausible" construction that would avoid a serious constitutional concern). This "canon of constitutional avoidance has no application in the absence of statutory ambiguity," *United States v. Oakland Cannabis Buyers' Coop.*, 532 U.S. 483, 494 (2001), and as *Amici* have shown, there is no ambiguity in section 2703(d). However, to the extent this Court finds that the statute is amenable to more than one reading, it is required to choose that

interpretation that would avoid any serious constitutional questions. *United States ex rel. Attorney General v. Delaware & Hudson Co.*, 213 U.S. 366, 407-08 (1909) ("[T]he rule plainly must mean that where a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, our duty is to adopt the latter.") (citation omitted).

2. The Mandatory Reading of 18 U.S.C. § 2703(d) Raises Serious Constitutional Questions About the Constitutionality of the SCA.

If this Court adopts the permissive reading of section 2703(d) and recognizes that the Magistrate Judge's decision to deny the Government's application was properly within her discretion, it will avoid the serious constitutional question of whether the CSLI at issue in this case—or even more precise location data that may be obtained with a D Order—is protected by the Fourth Amendment. On the other hand, if the Court adopts the Government's mandatory reading, it will run headlong into serious constitutional questions affecting the rights of every cell phone user.

As will be demonstrated in Section III, the government's use of the SCA to obtain the CSLI at issue in this case would raise serious constitutional questions but would indeed violate the Fourth Amendment. However, this Court need not hold that the Government's mandatory reading actually violates the Fourth Amendment in order to find that the Government's mandatory reading raises serious constitutional questions. Otherwise, the canon would "mea[n] that our duty is to first decide that a statute is unconstitutional and then proceed to hold that such ruling was unnecessary because the statute is susceptible of a meaning, which causes it not to be repugnant to the Constitution." *Almendarez-Torres v. United States*, 523 U.S. 224, 250 (1998) (Scalia, J., dissenting) (citation omitted).

The Court need only hold that the Government's reading raises serious constitutional questions.

Therefore, although the Government claims (without support) that the CSLI available in this case is extremely imprecise (Gov. Br. at 8 n. 6), that factual dispute is irrelevant to the constitutional avoidance question. The question is not whether applying the Government's mandatory reading of the statute in this case would be unconstitutional but whether that reading would raise serious constitutional questions in other cases. As the Supreme Court has held, the serious constitutional questions justifying application of the constitutional avoidance doctrine need not arise in the immediate controversy before the Court:

> It is not at all unusual to give a statute's ambiguous language a limiting construction called for by one of the statute's applications, even though other of the statute's applications, standing alone, would not support the same limitation. . . . [W]hen deciding which of two plausible statutory constructions to adopt, *a court must consider the necessary consequences of its choice.* If one of them would raise a multitude of constitutional problems, the other should prevail — *whether or not those constitutional problems pertain to the particular litigant before the Court.*

Clark, 543 U.S. at 380-81 (emphasis added). Regardless of whether the CSLI reflected in the Government's exemplar (Gov. App. 63) is accurate enough to violate a reasonable expectation of privacy, the fact that the Government is actually *seeking* in its application even more extensive CSLI,[3] combined with the fact the government has routinely sought even more accurate CSLI pursuant to § 2703(d),[4] is sufficient to warrant

---

[3] *See, e.g.*, Gov. App. 64 (Government's sealed and redacted application).

[4] *See, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) ("Also sought is information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites. . . . Armed with this information,

application of the constitutional avoidance doctrine here.

As the Government essentially concedes, the Supreme Court's location tracking precedents at least stand for the proposition that tracking which "reveal[s] facts about the interior of a constitutionally protected space" is "of constitutional concern." Gov. Br. at 29. Yet there is no evidence before the Court indicating that the extensive CSLI actually sought in the Government's application and in other cases, or the even more accurate GPS data available through some cell phone carriers, would not reveal just such details about the interior of Fourth Amendment-protected spaces, either now or in the near future.[5] Nor is there any evidence that even single-tower CSLI such as that reflected in the exemplar could never be so precise, considering the steady increase in the number of cell towers[6] and the use of new techniques for enhancing accuracy such as the use of "test phones."[7] Yet, the necessary consequence of a decision by this court to

---

collectively known as 'cell site data,' investigators are often able to locate suspects and fugitives.").

[5] The FCC has ordered cell phone carriers to have the following location capabilities by 2012 so that emergency responders can locate 911 callers: carriers using "network-based" (*i.e.*, CSLI-based) location methods must be able to locate phones within 100 meters for 67 percent of calls and 300 meters for 95 percent of calls, while those using "handset-based" (*i.e.*, CSLI-based) methods must be accurate within 50 meters for 67 percent of calls and 150 meters for 95 percent of calls. *See* 47 C.F.R. § 20.18(h)(1) (2008).

[6] *See, e.g.*, CTIA-THE WIRELESS ASSOCIATION, MID-YEAR 2008 TOP-LINE SURVEY RESULTS 9 (2008), <http://files.ctia.org/pdf/CTIA_Survey_Mid_Year_2008_Graphics.pdf> (showing sharp and continuing rise in the number of cell towers in the U.S.).

[7] *See Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J. L. & Tech. 307, 311 (Fall 2004) (describing how, in the Scott Peterson murder case, the prosecution's expert was able to pinpoint the defendant's past locations with

credit the Government's mandatory reading of section 2703(d) would be to allow the warrantless seizure of such information in future cases *regardless of its precision*, and therefore, on the Government's argument, *regardless of whether it is precise enough to be protected by the Fourth Amendment.*[8]

Such unintended consequences of serious constitutional import are exactly what the constitutional avoidance doctrine is intended to prevent, and are the reason that the accuracy of the specific CSLI at issue here is simply irrelevant when considering whether to apply that doctrine.

III. The Fourth Amendment Requires That the Government Seek a Warrant to Obtain CSLI.

This Court need not reach the question of whether CSLI is protected by the Fourth Amendment. However, if it does reach that question, the answer is clear: CSLI reveals information about the interior of spaces in which cell phone users possess a reasonable expectation of privacy and is therefore protected by the Fourth Amendment.[9] Further, individuals do not

---

CSLI by using "test runs" of his own phone to replicate Peterson's movements).

[8] Adoption of the Government's reading would also raise the specter of "dragnet surveillance" without warrants, the constitutionality of which has yet to be addressed by the courts and the threat of which is sufficient to justify application of the constitutional avoidance doctrine. *See United States v. Knotts*, 460 U.S. 276, 283-84 (1983) (noting that if the government were able to conduct twenty-four hour surveillance of any citizen's location, "such dragnet type law enforcement practices" may require the Court to reconsider its holding that drivers on public roads do not have an expectation of privacy in their automobiles' movements); *see also United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (noting potential for Fourth Amendment problems if government were able to engage in mass location surveillance of the populace using GPS tracking devices).

[9] The Fourth Amendment protects people, not places, so an individual may have a reasonable expectation of privacy even in matters disclosed to the public. *See Bond v. United States*, 529 U.S. 334, 338-39 (2000) (a police

knowingly expose their location information and thereby surrender Fourth Amendment protection whenever they turn on or use their cell phones.

A. CSLI Can Be and Routinely Is Used By the Government to Locate Individuals and Their Cell Phones Within Private Spaces.

Location tracking using unsophisticated "beepers" "falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance" from a public place. *United States v. Karo*, 468 U.S. 705, 707 (1984); *see also Knotts*, 460 U.S. at 282 (because "[v]isual surveillance from public places . . . would have sufficed to reveal all of these facts" that were revealed by the beeper surveillance, it did not implicate the Fourth Amendment). Government access to CSLI reveals such information and therefore falls within the ambit of the Fourth Amendment.

CSLI reveals information about the interior of private spaces like homes and pockets, information that could not be obtained through surveillance from a public place. As the Court in *Karo* held,

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article — or a person, for that matter — is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.

---

officer's exploratory squeezing of soft-sided luggage on a bus is a search, even though a traveler knows that members of the public may touch his baggage when putting their own luggage on the rack).

468 U.S. at 716. Yet CSLI, even when imprecise, reveals the location of individual and her cell phone even when withdrawn from public view, as two examples — one actual, one hypotethical — will demonstrate.

First, the Government uses CSLI to place individuals at their homes and in other constitutionally protected spaces. The FBI's cell tracking expert has testified in this Circuit that CSLI is reliable evidence that a suspect is at his or her home. *See United States v. Sims*, Eastern District of Pennsylvania Case No. 06-674, November 13, 2007 Testimony of William Shute, included as Exhibit A (hereinafter "Shute Tx").[10] This testimony belies the government's claim that CSLI "is far too imprecise by any measure to intrude upon a reasonable expectation of privacy." Gov. Br. at 26.

In *Sims*, FBI Special Agent and CSLI expert William Shute testified that he has used historical cell site information to locate fugitives almost 150 times. Shute Tx at 17. The agent did not testify that CSLI conclusively pinpoints the suspect's location, but he did testify that the jury can and should rely on the CSLI evidence to conclude that a suspect is in a home. For example, Shute testified that CSLI showed that the phone subscriber was likely at her home during a particular point in time:

> However, it is highly possible that Ms. Andrews was at her home, that cell site is only 60 yards from her house . . . . So, it is safe to conclude that Ms. Andrews, if in fact she is in possession of the phone, was in the vicinity of her home during that particular call.

---

[10] The CSLI in *Sims* was call detail records from Sprint-Nextel, the same company from which the Government seeks records in this case. *See* Shute Tx at 12; Government's Memorandum of Law In Support of Request for Review of April 21, 2008 (Docket No. 11) at 2.

Shute Tx at 20; *see also id.* at 21 ("It is highly possible that Ms. Andrews was at her home."). Later in the day, Shute placed the phone at another private location, noting "a great possibility that the phone is right in the middle on that overlap area," an area where another suspect's residence was located. Shute Tx at 21-22. The agent further testified:

> [W]hat I want to show between the hours of approximately 12 and 7, the Nextel cell phone bounced between those two cell phone towers. As I said, this is consistent with the phone being stationary in the overlap of the two cell site sectors, and what I wanted to show you is within that area is Tony Thompson's residence . . . .

Shute Tx at 25. Shute's testimony contradicts the Government's assertions that historical CSLI cannot be used to identify a suspect's location. *See, e.g.* Gov't Brief at 35. Rather, Shute says that the data is accurate enough to regularly apprehend fugitives and that a jury can conclude from CSLI that calls were made from the Andrews and Thompson residences. Shute Tx at 17, 20-22, 25. Shute's testimony also contradicts the Government's claims that CSLI cannot be used to conclusively determine that a cell phone is in a particular area. *See, e.g.,* Shute Tx at 17 ("It would be somewhere in that area for sure."); *id* at 19 (stating that the phone was "very, very close to the bank."); *id.* at 27 (Q: "Where was the phone? A: "In the highlighted area."); *id.* at 28 ("The phone is actually in a very smaller area [than eight blocks], in that overlapped area.").

Shute's testimony confirms, as *Amici* argued below, that the Government will use the fact that the suspect's phone contacted the cell tower nearest his home to infer he is home, nearest the narcotic's kingpin's

house to infer that they are together, nearest the drop off point to argue that he was present when the contraband was delivered. Indeed, the Government expects such information to support a finding of guilt beyond a reasonable doubt. For the Government to claim that CSLI is far too inaccurate for it to be used for the very purpose it does use it — to locate people within their homes — is disingenuous at best. If it is accurate enough for the jury, it is accurate enough to implicate the Fourth Amendment.

An additional hypothetical further demonstrates how imprecise CSLI reveals information about the interior of private spaces that was never exposed to the public. Imagine that the police are visually surveilling "Bob." Bob has a cell phone, and unlike the multi-gallon chemical drums to which beepers were attached in *Karo* and *Knotts*,[11] Bob can conceal his cell phone in public by carrying it in his pocket. However, on this occasion, when Bob enters his office in Manhattan, he happens to be on a call, and the police therefore know that the phone has entered the office. Later, Bob leaves the office with the phone in his pocket and travels to his house in Brooklyn with the police following. When he arrives inside his home, he then pulls the phone out of his pocket and makes a call.

As far as the officers could know from visual surveillance, *the cell phone never left Bob's office.* Yet even the most inaccurate CSLI directly reveals that the cell phone had traveled from Manhattan to Brooklyn. It would therefore indicate that the phone was no longer in Bob's office, had been carried in Bob's pocket, and was now in his home, all private spaces. Visual surveillance alone would have revealed none of this; only physical searches of Bob's home, office, or person would have. Therefore, the

[11] *Knotts*, 460 U. S. at 277 (1983) (five gallon can of chloroform); *Karo*, 468 U.S. at 714 (five gallon can of ether).

information about the phone revealed by the CSLI is protected under *Karo* and *Knotts*.

The police may not consider the cell phone's location — specifically, the fact that it was moved into Bob's home — to be "particularly private or important, but there is no basis for saying it is not information regarding the interior of the home." *Kyllo v. United States*, 533 U.S. 27, 35 n. 2 (2001). Rather, "[t]he Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." *Id.* at 27, 37-38 (holding that Fourth Amendment protection does not hinge on whether the information revealed is an "intimate detail").

The Government may also argue that the CSLI only confirmed what they might have inferred from surveillance in public, *i.e.*, that Bob was carrying his phone. However, confirming this inference about the location of the phone triggers the Fourth Amendment. *Karo*, 468 U.S. at 715 ("Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises."); *see also Kyllo*, 533 U.S. at 35 n. 2 (finding it "quite irrelevant" that information obtained through a thermal imager about the heat inside the home may have been perceived by observers from public without the use of technology). Conversely, the fact that even imprecise CSLI *enables* the Government to make inferences about the location of the phone and its user is enough to trigger the Fourth Amendment. *See Kyllo*, 533 U.S at 36 (rejecting "the novel proposition that inference insulates a search," noting that it was "blatantly contrary" to the Court's holding in *Karo* "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home.").

Because the Government can and does use CSLI to infer the specific location of cell phones within protected spaces, such information is protected under the Fourth Amendment regardless of its technical precision. This conclusion is bolstered by the rudimentary nature of the technological monitoring done in those cases. Beepers are "unsophisticated, and merely emit[] an electronic signal that the police can monitor with a receiver. The police can determine whether they are gaining on a suspect because the strength of the signal increases as the distance between the beeper and the receiver closes." *United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004); *see also Karo*, 468 U.S. at 708 ("the beeper equipment was not sensitive enough to allow agents to learn precisely which locker the ether was in . . ."). Similarly, the thermal imaging technology at issue in *Kyllo* was "a non-intrusive device . . . [that] show[ed] a crude visual image" of the heat radiating from a house and did not reveal any "intimate details" about the interior of the home. *Kyllo*, 533 U.S. at 30; *see also id.* at 36 ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."). Even so, the monitoring at issue in *Karo* and *Kyllo* — and the CSLI at issue here — nevertheless reveals facts about the interior of protected spaces that would not have been revealed solely by surveillance from public, and is therefore subject to the Fourth Amendment.

B. A Cell Phone User Does Not Knowingly Expose Her Phone's Location Whenever She Turns It On or Uses It.

A cell phone user does not knowingly expose the phone's location, nor is a wireless provider a party to a user's cell phone communications. On these grounds, *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), upon which the Government relies, are

easily distinguishable. *Miller* did not deny Fourth Amendment protection solely because bank records "are not [the customer's] 'private papers'" but instead "the business records of the banks" in which a customer "can assert neither ownership or control." Gov. Br. at 26, quoting *Miller*, 425 U.S. at 440. The Government ignores the Court's basis for its holding in *Miller*: "*Banks . . . are . . . not neutrals* in transactions involving negotiable instruments, *but parties* to the instruments," and the records "pertain to transactions to which *the bank was itself a party*." 425 U.S. at 440, 441, quoting *California Bankers Assn. v. Shultz*, 416 U.S. 21, 48-49, 52 (1974) (emphasis added). In contrast, a cell phone provider is not a party to its customers' transactions (*i.e.*, their phone calls); rather, it is indisputably a provider of an "electronic communication service" which "provides to users thereof the ability to send or receive wire or electronic communications" to others. 18 U.S.C. § 2510(15). Such providers are indeed "neutrals," intermediaries between cell phone users rather than a party to their calls.

The Government compounds its error by claiming that cell phone users voluntarily convey their CSLI to the cell phone provider, as the bank customer in *Miller* conveyed checks and deposit slips to the bank, or the telephone customer in *Smith* conveyed dialed numbers to the phone company. Gov. Br. at 27-28. Yet this analogy is wholly inapt: in both *Miller* and *Smith*, the relevant documents and dialed numbers were directly and knowingly conveyed to bank tellers and telephone operators or their automated equivalents. *See, e.g., Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information . . . . The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the

subscriber."). Put simply, the phone customer knew what numbers he was exposing to the phone company; the bank customer knew what documents he was exposing to the bank.

The exposure of CSLI to a cell phone provider is nothing like the direct conveyance of phone numbers to an operator or bank documents to a teller. As the Magistrate Judge correctly held, "CSLI is not 'voluntarily and knowingly' conveyed (certainly *not* in the way of transactional bank records or dialed telephone numbers); rather, the information is automatically registered by the cell phone." M.J. Order, 534 F. Supp. 2d at 615 (emphasis in original), citing *United States v. Forest*, 355 F.3d 942, 949 (6th Cir. 2004); *see also In re Application for Pen Register and Trap/Trace Device With Cell Site Location Auth.*, 396 F. Supp. 2d 747, 756-57 (S.D. Tex. 2005) (CSLI is transmitted by the phone "entirely independent of the user's input, control, or knowledge"). When a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all. *See, e.g., Forest*, 355 F.3d at 949. And a caller most certainly does not voluntarily provide the registration information that the phone automatically sends to the phone company every seven seconds whenever the phone is on, without notice to or control by the user. *See* M.J. Order, 534 F. Supp. 2d at 590 (describing automatic registration process); *see also* Gov. App. 64. Indeed, the average cell phone user does not even know the location of the nearest cell phone tower or which tower their phone may be registering with or communicating through. Nor does this information appear in the typical cell user's bill, a critical fact in *Smith*. *See Smith*, 442 U.S. at 742 ("All

subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.").[12]

In sum, the CSLI at issue is easily distinguishable from the information at issue in *Miller* and *Smith*: cell phone users simply do not voluntarily expose their location whenever they make calls and receive calls to which the provider is not a party, nor do they do so merely by turning on their cell phones. *Karo* and *Kyllo* control, not *Miller* and *Smith.*

IV. If the Court Believes That the Accuracy of the CSLI at Issue is Relevant, It Must Remand for an Evidentiary Hearing.

The accuracy of CSLI at issue is irrelevant to determining whether the Government's reading of the SCA raises serious constitutional questions, *supra* at Section II.D.2, irrelevant to whether it is protected by the Fourth Amendment under *Karo, Kyllo*, *supra* at III.A, and irrelevant to whether *Smith* or *Miller* applies. However, to the extent the Court disagrees with *Amici* and believes that the accuracy of the CSLI at issue here is relevant to any of these questions, it must remand for a factual hearing.

The Government admits that hard evidence about the accuracy of CSLI is absent from the record. Gov. Br. at 32. If that information is relevant to deciding this appeal, the Court cannot, as the Government suggests, resolve this serious constitutional question based on turn-of-the-century FCC reports that are woefully out-of-date considering the rapid advance of cell phone technology and in particular the rapid proliferation of cell phone towers, which necessarily increases CSLI's accuracy. *See* Gov.

[12] To the extent the Government disputes what the average cell phone user does or does not realize or what her subjective privacy expectation may be, remand for an evidentiary hearing would be appropriate. *See infra* at Section IV.

Br. at 34 n. 19 (suggesting that the Court take judicial notice of statements by the FCC in 1999, 2000, and 2001 concerning the accuracy of CSLI), *but see* CTIA-THE WIRELESS ASSOCIATION, MID-YEAR 2008 TOP-LINE SURVEY RESULTS 9 (2008), located at <http://files.ctia.org/pdf/CTIA_Survey_Mid_Year_2008_Graphics.pdf> (showing how the number of cell towers in the U.S. tripled between 1999 and 2008, from 74,157 to 220,472). Nor can this Court rely on the Government's otherwise unsupported assertions about the accuracy of CSLI generally, especially in light of Agent Shute's testimony to the contrary. Therefore, this Court must remand for an evidentiary hearing if it finds that CSLI's accuracy is relevant and refuses to credit the Magistrate Judge's finding.

CONCLUSION

For the foregoing reasons, the decision of the District Court should be affirmed.

DATED: March 16, 2009

By Witold Walczak

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Attorneys for *Amici Curiae*

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 6,976 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 proportionally spaced typeface using Microsoft Word 2004 version 11 in Times New Roman, 14-point font.

DATED: March 16, 2009

By Witold Walczak

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Attorneys for *Amici Curiae*

CERTIFICATE OF SERVICE

I certify that, on this 16th day of March, 2009, the BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, ET AL., IN SUPPORT OF AFFIRMANCE OF THE DISTRICT COURT was served on all parties via electronic filing. And that, pursuant to Third Circuit Rule of Appellate Procedure 25.1, ten (10) paper copies were delivered to a third-party commercial carrier for delivery to the Clerk of the Court within three calendar days.

DATED: March 16, 2009

By Witold Walczak

Witold J. Walczak
ACLU of Pennsylvania
313 Atwood Street
Pittsburgh, PA 15213
412-681-7864
vwalczak@aclupgh.org

Attorneys for *Amici Curiae*

Exhibit A

U.S. Department of Justice
United States Attorney
Eastern District of Pennsylvania

ALEXANDER T.H. NGUYEN
Direct Dial (215) 861-8637
Fax (215) 861-8498
Email Address: alexander.nguyen@usdoj.gov

615 Chestnut Street
Suite 1250
Philadelphia, Pennsylvania 19106-4476
(215) 861-8200

February 4, 2009

Via Electronic Mail to mark_wilson@fd.org

Mark T. Wilson
Defender Association of Philadelphia
Suite 540W, The Curtis Center
601 Walnut Street
Philadelphia, PA 19106

Re: United States v. Brown
Criminal No. 07-743

Dear Mr. Wilson:

In follow up to our telephone conversation of today, I am enclosing William Shute's testimony from United States v. Sims, No. 06-674 from this district. His testimony is Bates-labeled CBF431 through CBF460.

Please call me if you have any further requests or additional questions. Thank you.

Sincerely yours,

LAURIE MAGID
Acting United States Attorney

s/ Alexander T.H. Nguyen
ALEXANDER T.H. NGUYEN
Assistant United States Attorney

Enclosure

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

UNITED STATES OF AMERICA	:	
	:	CRIMINAL ACTION
vs.	:	
	:	
AESHA SIMS, TONY THOMPSON, AND SABINA ANDREWS	:	NO. 06-674
	:	
	:	
Defendants	:	

Philadelphia, Pa.
November 13, 2007

BEFORE: HON. STEWART DALZELL, J.
And a Jury

TRIAL - FIRST DAY

TESTIMONY OF WILLIAM SHUTE

APPEARANCES:

For the Government: OFFICE OF THE U.S. ATTORNEY
BY: ANTHONY WZOREK, ESQ.
And ALEX NGUYEN, ESQ.
Assistant U. S. Attorneys
615 Chestnut Street
Suite 1215
Philadelphia, PA 19106

For the Defendant: ROBERT B. MOZENTER, ESQ.
Aesha Sims
121 South Broad Street
Suite 500
Philadelphia, PA 19107

For the Defendant: DAINE A. GREY, JR., ESQ.
Tony Thompson
320 North 18th Street
Philadelphia, PA 19103

For the Defendant: JOSEPH C. SANTAGUIDA, ESQ.
Sabina Andrews 121 South Broad Street
Second Floor
Philadelphia, PA 19107

SIDNEY S. ROTHSCHILD
Official Court Reporters
Room 1234 - U.S. Courthouse
601 Market Street
Philadelphia, Pa. 19106
(267) 738-8713

Proceedings recorded by mechanical stenography, transcript produced by computer.

WILLIAM B. SHUTE, SWORN

THE DEPUTY CLERK: Would you state and spell your full name for the record?

THE WITNESS: William B. Shute, S-H-U-T-E.

THE COURT: Agent Shute, pull that microphone close and speak into it.

Proceed, Mr. Wzorek.

MR. WZOREK: Thank you, your Honor.

DIRECT EXAMINATION

BY MR. WZOREK:

Q. How are you presently employed?

A. By the FBI, the Federal Bureau of Investigation, the FBI.

Q. How long have you been employed by the FBI?

A. Well, 12 years, approximately eight as an agent.

Q. In your work, do you use cellular telephone technology in your investigations?

A. Yes, I do routinely, probably everyday.

Q. About how long has that been going on?

A. Since I have been in the FBI.

Q. Have you received any special training regarding cell phone technology?

A. Yes, I have. I received training from the FBI regarding cellular telephone technology and also have been sent to several courses by a private company

known as ETS, Emerging Technology Support is the company. It is a company that is comprised of former military and other Government workers that provide training and cellular technology radio frequency theory, those concepts, they provide that training back to other Government entities.

Q. Have you also had training by other cellular telephone companies as well?

A. Yes, I have routine interaction with cell phone companies in the Philadelphia metropolitan you know T-Mobile, Cingular, now AT&T, Sprint, Verizon Wireless and particularly a lot with Nextel.

Q. Can you summarize as closely as you can what areas of training you have gone into with these companies, what types of training?

A. Well, we have talked about radio frequency theory because essentially a cell phone is a two way radio transmitter, we have gone into the various technologies because out of those five cell phone providers that I just mentioned to you, they operate in three different technologies, T-Mobile and AT&T are a GSM network. GSM stands for global standard mobile communications, that's one technology. Sprint and Verizon Wireless is another technology called CDMA, code division multiple access, a fancy name for it,

but it is important to note it is a different technology. And, then you have Nextel which is a technology called IDEN, integrated digital enhanced network. All three different technologies pretty much acting in the same fashion.

Q. Have you been certified as an FBI instructor in historical cell site analysis?

A. Yes, I have been certified as an FBI instructor, yes, particularly, my focus is usually cell site, historic cell site analysis.

Q. What exactly does it include?

A. It is kind of a concept that hasn't been around all that long. What it is, it is taking the historical records of a person's, what we call the detail records and the cell site information and taking them -- creating an analysis of where that phone was at each particular call and then laying that geographically on to some type of a mapping program. It used to be years ago we had to tape maps together to do it, but now we can do it all with computers.

Q. How is it you find out where the phone is located, what are you using?

A. I'm sorry?

Q. What are you using to find out where the phone is located when a call is made?

A. We use in particular the column known as the cell site column, the originating or the terminating cell site.

Q. Also called cell towers?

A. Cell towers.

Q. Do you train other agents in the FBI as part of your expertise?

A. Yes, I have been to 25 different cities to train the various agents and various aspects of this type of technology. I have routinely instructed county detective schools in the Philadelphia metropolitan areas and then I was asked by FBI lawyers to create a curriculum, three day course that teaches these concepts to other agents and police officers across the country. So, we have done two of those so far. We are doing another conference in two weeks here in Philly.

MR. WZOREK: Your Honor, I'll submit Agent Shute as an expert in historical cell site analysis.

THE COURT: Expert in historical?

MR. WZOREK: Cell site analysis, your Honor.

THE COURT: Cell site.

MR. WZOREK: Analysis.

THE COURT: Okay. Any voir dire?

MR. SANTAGUIDA: I wouldn't know how to

cross-examine him. I have to accept him.

THE COURT: No objection?

MR. GREY: No objection.

THE COURT: I will therefore certify that Special Agent Shute is an expert in historical cell cite analysis.

BY MR. WZOREK:

Q. Tell the ladies and gentlemen of the jury, in as simple terms as possible how a cell network works?

A. We will try. A cellular network is kind of a complex matrix of a lot of different parts operating, but in the essence of simplicity we can basically describe it in this fashion:

You have a cellular telephone which interacts with cell phone towers, okay. Those cell phone towers are also known in the engineer's world as base stations. So a cell phone tower is the same as a base station.

You have cell phone towers or base stations controlled by base station controllers. In a given geographical area there could be numerous base stations all reporting to an area known as a LAC, location area code. So if you want to think of it this way, an area location code could be anywhere from 100 to 125 cell phone towers operating in this one

area known as a LAC, that's an important term for later on.

The LAC then is controlled by something known as the mobile switching center or they call it a switch, it is at this location at the switch, where all of the types of data are recorded, and one of them is normal billing procedure data.

Now what is the data and why is it recorded? We will get to that in a second.

It's important to know about a cell phone, that a cell phone although it is kind of a cheaply, easily made device is actually a very smart device. The one thing that I want you to take away about cell phones is that cell phones are a lot like children, they won't talk to strangers. At any given time, your cell phone knows the cell site sector it likes the best. If you want to think of a cell phone tower, it has three different sectors, and in the case of Nextel, if you were to look at the face of a clock, they would generally be oriented from 12 to 4, 4 to 8 and 8 to 12. Those are the three cell sectors that Nextel orients their towers.

And what is happening is that the call, okay, when a phone call comes through, it gets paged through that entire LAC, that location area code. So, if your

phone is sitting there idle, your wife or husband calls you, the phone call comes in, it is paged throughout that entire LAC, it could be 25, it could be 100 towers, and the phone is sitting there idle and the phone hears this page, it pages, it is basically a silent scream, screaming where are you? Where are you? When the phone responds, when it hears that, it responds with a paged response. Where does it respond to? The phone responds to the cell site sector that it sees strongest. When it happens, it goes through a series of interactions which happens instantaneously and then that cell phone call is placed up on that cell site sector. What happens is it sees the cell site sector it likes the best. It can also see up to six other tower sectors in the area, okay, it is important to take that into consideration.

It stacks and racks them. When your phone is sitting there idle, it sees the cell site sector it likes the best, but it also sees up to six additional sector that it could go to if it needed to.

Let's get back to what the data is that is being recorded. The data being recorded at the switch is the global cell site ID. Global cell ID is a fancy term for a cell site, so when that call gets placed up on that particular cell site sector, okay, what

happens is it records that as the originating cell site. The phone goes through the series of the conversation. When the call is terminated, it also records that as well.

Why does it record that? It records it for three main reasons.

One, for maintaining your call quality, really is one of the biggest reasons.

For maintaining calls from tower to tower. How else would you be able to drive your car and still stay on the cell phone.

Lastly and probably most importantly is for billing purposes. I think if there is one thing that everybody can understand, a cell phone company is in business to make money. Not too long ago there were roaming charges. This is how the phone company would know if you are not in your home area. It keeps track of you down to that, down to the cell site, the LAC of cell phone towers and the cell site sector.

What is happening when law enforcement asks for that data via Court order, whatever the legal process we ask it, that's what we are asking, the normal billing procedure, the normal business records that say in this case Nextel uses to keep track of the cell phone in order to provide its service. So that

is kind of how the cell phone network works and how the data is then acquired by law enforcement.

Q. Let me ask you a few stupid questions.

Is it fair to say when you use the cell phone, it bounds of the nearest cell phone tower, is that generally the case?

A. Generally the nearest one at that point, the signal strengths from that cell phone tower is so great.

Q. As I'm moving, as you say in the car and I am driving down Route 1 or the Schuylkill Expressway, that tower may change with me as I'm still on the phone, going down the road, is that correct?

A. That's true. It even changes when you are not on the phone, it continually does that stacking and racking that I am talking about. At any given time, your phone knows the tower that is the strongest, not just the tower but that sector that I'm talking about and then it knows, as I said up to six others. So if it sees the next tower as being the second strongest, it stacks it there, the next one, it stacks it there. It gives it in order in which it could bounce to if needed to. It reports that back to the cellular network, that's how the network knows where to switch the call to.

Q. If I understand you correctly, you can use the information you received to basically locate where a cell phone is within a range, when a phone call is made, is that correct?

A. Definitely.

Q. More specifically related to this case, did you review the records for a cell phone number 267-688-1610?

A. Yes, I did.

Q. And did that belong to Sprint Nextel?

A. Yes, in particular it was the Nextel portion of Sprint Nextel.

Q. Did you also obtain from those records, I believe you called them earlier the call detail records, is that correct?

A. Yes, it was the call detail records to include cell site information.

Q. What exactly is that, does that give you the cell towers that are being struck?

A. Yes. In a few minutes we will actually see some of the call records. It gives you the date, the time of the call, the phone number that is being dialed. It will tell you the duration of the call, I think they show it in seconds. Then it will give you originating and terminating cell site, that means it

will show you the location of where the phone was at the moment that the call was initiated. When like I said, the network is screaming to where are you, it gets placed up on that call, that is what you are seeing as originating cell site. Where you see terminating cell site, wherever that cell site sector was when it ended.

Q. You made up a power point based on the information you received as a result of your analysis, is that correct.

A. I thought that was the easiest way to present it.

MR. WZOREK: We have it marked as Government Exhibit 16.

May we play that for the jury at this point?

Q. Agent, you have with you -- I see something in your hand, what's that?

A. It is just what we call a remote clicker, it advances the slides.

Q. You can do that without further action on our part?

A. Yes.

Q. Tell the jury what you presented here?

A. This is a cover sheet here of what I normally do when I present these things for court purposes, and it then what we will do is I want to show you the typical

layout, the way that Nextel describes it. What you see there is if you were looking straight down on to the cell site sector, this is what a tower would look like.

What I want to do is read this to you. It says: That this cell site analysis is based on the layout of the Nextel cell phone towers. Most cell towers in Nextel's network are designed to have a three sector layout. Each cell site and cell site sector are unique and the numeric code assigned to each sector is not duplicated anywhere else on the cellular network. Most Nextel towers are oriented in this fashion, with sector one being to the northeast face sector, highlighted in yellow. Sector two being the southern face, highlighted in red and sector three being the northwest face, highlighted in blue.

Q. So you have indicated each cell site has a particular code to it that's unique to it, is that correct?

A. Correct. If you look down there, I will point with this laser pointer, this is why I said generally 12 to 4, 4 to 8 and 8 to 12, that's what you will see on the cell site analysis.

The next slide just indicating that all the calls displayed on this particular analysis I have

done took place on Friday, June 9, 2006, between the hours of 7 a.m. and 7 p.m.

Q. That's based on the records that you reviewed, is that correct?

A. That's correct, the only records that I reviewed.

What we have here is the call detail records to include cell site information for the particular cell phone 267-688-1610.

What you see there is you have columns for customer PTN, customer personal telephone number, the date, you see the call initiation time, the duration in seconds as I said. It tells you the type, is it inbound or outbound call. Whether or not the call was forwarded. Typically the calls are forwarded when they go to voice mail sometimes. If it was a 911 call, if it was an international call. Then you get into the initiating cell site and terminating cell site. So that right there what you are seeing if you want to look at the very top cell site, you can see right there the last set of digits is 4108 is the LAC and 14088 is the cell site. So, it is part of the global cell ID I'm talking about. It is the last two parts, that's what Nextel provides you, the LAC and the cell site, so it gives you the region and then the cell site tower, down to the cell site sector is what

they are providing you with there.

So what I have done here is taken a group of calls. So in this case I have taken from 7:06 a.m. through 7:37 a.m., and take that time frame and took those cell sites and plotted them on the map so you can all see it. Primarily we are seeing the same cell site 14088 and then also in this general vicinity right here is the area, the geographical area represented by that particular cell site.

Q. What do you mean by that?

A. Well what happens is 14088 is in Nextel's engineer's list, which is their master list that they provide to us.

They have cell site, well, LAC 4108 and cell site 14088 cell site sector two. Nextel, what they do is give each sector its own numeric code, that numeric code right there is equivalent to sector two displayed in the highlighted yellow area.

Q. I see red dots, about 7 or 8 of them across this map, what are they?

A. They are the other Nextel towers in the area. One of the reasons that it is usually very important to display that is to be able to show the Court the approximate range. When I built this analysis, I am always more generous towards the area where the phone

could be. In fact, if I was looking for somebody for say fugitive purposes, which is, I have used this well over 100 times, probably close to 150 times to locate people, I wouldn't even be - - I wouldn't span that geographical area that far. I wouldn't look for the person -- I would look for the person closer to the cell site. In the essence of being fair in court purposes, I wanted to show the greatest possible range of where that phone could be in that general area.

Q. Why is that in the lower section from the 4 to 8 I guess, it is colored in?

A. Why is that?

Q. Yes.

A. That is representative of that cell site sector of which cell site 14088 is facing, where callers would be if they were using that cell site sector.

Q. Sort of summarizing, if you went back just having some phone number bounce off that cell tower you see right in the middle of the circle, it could be theoretically in that circle. Once you get the additional information, you can restrict it to a certain area, is that correct?

A. That is correct, being fair, it would be somewhere in that area for sure.

Q. Again those are the calls that you had

highlighted before, the 7:06 all the way through the first four calls we saw, is that correct?

A. That is correct.

Q. Continue, please.

A. Then the next slide just depicts where Sabina Andrews' work location is.

In this particular spot, it is Inter-Community Action Incorporated at 6710 Ridge Avenue.

Also what plays a part in cell phone towers is geographical area and this particular area, Roxborough, Manyunk is very hilly. Where you see the cell site down here all the way to the bottom of where that box is, if you are familiar with the area, and I am, that is much lower than the actual cell site that the phone is being used on.

So, the actual cell site down at the bottom would have been lower than the location of where the business is.

So, it is more likely that the phone would have seen 14088 as the strongest tower at that point. Okay. Then the next sets of calls is right here.

Q. Let me stop you before you get too much further.

You talked about these different columns, there's a column about two-thirds of the way over called caller and call PTN.

A. Correct.
Q. What is that?
A. Well, depending upon if you look at the column that says type, whether it is inbound or it is outbound, if it is an inbound call, then that's going to show who the person was that was calling. If it is an outbound call, it will show the reverse. That's what that is.
Q. Okay.
A. So the next calls are both at 7:50 a.m., and it what we are showing here, these two calls and where they are actually at. As you can see there are three separate LACs, and cell site sectors 19284, 37638 and 2722. That would be representative of this area right here. Those in that order is the way that those calls were -- cell sites were hit.
Q. Let's go to the circle up on top, you have a blue flag outside of the circle at 417 West Olney Avenue, the Wachovia Bank there, is that correct?
A. That is correct.
Q. The first call was made somewhere in that area near that bank, is that correct?
A. Very, very close to the bank, sure.
Q. Then how do you interpret the differences of the circles, it means the person is moving or what?

A. Yes, it means, I won't speculate because I don't know the route that was taken, but it moved in that kind of south, southeasterly direction, the calls, as the calls were being recorded.

Q. There's another little blue flag right above the third circle, down toward the right hand section. Do you know what that is on D Street?

A. I believe that is Sabina Andrews' home residence, I believe.

Q. Would you continue, please.

A. Then we will show this particular call at 8:57 a.m., which utilizes cell sites 20926 and 37674. It was -- let me go back, 17 second call. It was initiated on this cell site sector here but then terminated right there.

In the case of like this, you know, I don't speculate where the person was. I just show you where the cell site sectors are.

However, it is highly possible that Ms. Andrews was at her home, that cell cite is only 60 yards from her house, approximately maybe 60, 70 yards and with the strength that close, the cell phone would -- I know this because I do it all the time with my own personal engineering hand set.

MR. SANTAGUIDA: Objection to that, Judge.

THE COURT: I agree. Just answer the question, sir.

THE WITNESS: Sure, it would -- the cell phone would probably seek both sectors equally the same because of the proximity to the tower.

Q. Would you continue, Agent.

A. Sure. So, it is safe to conclude that Ms. Andrews, if in fact she is in possession of the phone, was in the vicinity of her home during that particular call.

Then we have the next two calls, 9:04 a.m. 9:06 a.m., and these are the cell sites being utilized. As you can see, one originating then another terminating. On the second call, there's another originating and another terminating. Basically, it is representative of this, these cell sectors here, which again shows me that the phone is on the move, kind of heading in a southwesterly direction.

Then we look at this call at 9:28 a.m., which is a 21 second phone call, initiated on 37032 and it terminated on 2747. So, initiated here, terminated here. Because it was only a 21 second call, it is a great possibility that the phone is right in the middle on that overlap area, that happens

frequently when a phone call - - a phone initiates on one but terminates on the other, it would be right smack in the middle of the two cell sites because again the phone is continually stacking and racking and one second it may see 3730 as the strongest but 8 seconds later it can see 2747 as the strongest signal. Just solely based on movement and where the phone is at that time.

Q. That area is somewhere west of Broad Street, west of South Broad Street, is that correct?

A. Yes, correct, in South Philadelphia, on the west side of Broad Street.

Q. Okay. There's a blue flag over toward the left hand side of that chart, is that the information you had received, Reed Street, Aesha Sims' residence, is that correct?

A. That is correct. It was communicated to me that address was a significant location. I just plot that to show that the phone was approximately in a half mile --

MR. SANTAGUIDA: I'll object to the term "significant".

THE COURT: Okay, the objection is sustained.

BY MR. WZOREK:

Q. That is the address you were given?

A. That is correct.
Q. Can we get to the next slide, please.
A. Sure. In the next set of calls, it is approximately an hour time frame from 9:54 until 10:56 a.m. What you see here is all the same cell sites over and over again throughout that entire hour period, cell site 20946. When you see these types of calls consistently on the same cell site throughout a time frame like this, for example, in an hour time frame, it usually means that the phone is very close to the tower. And in this case, that is representative of that cell site sector and I'm just displaying where Sabina Andrews' residence is.
Q. Again you said that was about 60 yards?
A. It was approximately 60 to 70 yards from the actual tower, extremely close. The power from that cell phone tower would be so great, it would be difficult to go anywhere else.
Q. Go to the next slide, please.
A. Then for the next seven hours, Sabina Andrews consistently utilized two Nextel cell towers.
MR. SANTAGUIDA: I object to who was utilizing it.
THE COURT: It is Sabina Andrews', the telephone that is registered to Sabina Andrews?

JUROR: Correct.

THE COURT: With that understanding, please proceed.

THE WITNESS: It is important to note that it is the phone not - - I cannot say who had the phone in their possession.

But, that phone, consistently used two Nextel cell towers which overlap each other.

And, as you will see it for the next seven hours, beginning at 12:12 p.m., so, you will then see 14258 and 37884 consistently throughout these records.

Again, this set of records here from 1 o'clock through 2:37 p.m., you are seeing the same cell site sectors over and over. Sometimes it originates on 14258, sometimes it terminates on 37884. Again all the way through 5 o'clock, you are seeing 14258 and 37884.

From my experience and utilization of this technology, that is extremely consistent with the phone being somewhere in the middle of the two cell site sectors, when you hit consistently over a seven hour period between two phones. It is not to say that the phone wasn't moving but this is very consistent with the phone being in one location but utilizing two

separate towers.

And, that is 14258, the general geographical area and then you can see the other cell site sectors in the region. You also see 37884 and, whenever I use this to locate someone, I generally believe that they are in the overlap and what I want to show between the hours of approximately 12 and 7, the Nextel cell phone bounced between those two cell phone towers. As I said, this is consistent with the phone being stationary in the overlap of the two cell site sectors, and what I wanted to show you is within that area is Tony Thompson's residence, 3111 North 9th Street, Philadelphia, Pennsylvania.

Q. Where the blue flag is?

A. The blue flag location is Tony Thompson's residence.

Q. That's the last slide, am I correct?

A. That is correct.

MR. WZOREK: No further questions, your Honor.

THE COURT: Cross-examination.

MR. GREY: I have no questions, Judge.

CROSS-EXAMINATION

BY MR. SANTAGUIDA:

Q. Is there anything illegal about any of this that

you told us?
A. I don't understand.
Q. Well, I mean, what you have explained to us you are trying to track where a particular phone is, when a call is about, either being made to that phone or being on - -
A. That's not what I am saying.
Q. That's not what you are saying?
A. I'm not tracking anything, the cellular network has to keep track of the phone to provide the phone with cellular service.
Q. I understand. What you are here trying to do is trying to explain somehow I guess the location of the phone in question, is that correct?
A. Yes.
Q. Is that right?
A. Yes.
Q. Now, again I have no clue of what you are talking about but it seems to me that you can only, you are not sure where the phone is, you can only guess an approximate area?
A. The area highlighted.
Q. The area highlighted. How many block area?
A. Well, in this, each call is different because it pertains say for example, the cell site you see on the

screen right now, 14258, you can't answer whether a phone, what's the particular range of the particular tower. It has to do with each call by call basis, meaning where are the other calls. As you can see that cell site sector is from 12 to 4. It depends on where the other cell sites in that northeast region are in comparison to 12458 so in this --

Q. That's a lot of double talking. Where was the phone?

A. In the highlighted area.

Q. What's the highlighted area, what street?

A. Sir, you have eyes, it is right there on the screen.

Q. Don't you know?

A. Sure I do.

Q. Tell me?

A. On Lehigh Avenue.

Q. Where?

A. West of 13th.

Q. What hundred?

A. It looks like somewhere between 1300 and 1400 Lehigh.

Q. You don't know where?

A. That's where the cell site tower is.

Q. Where the tower is. Where is the phone?

A. In the Northeast region, approximately three quarters of a mile from that tower.
Q. Three-quarters of a mile?
A. In the area highlighted.
Q. That's about eight blocks?
A. Well, yes, it is, except for the fact that the cell phone also utilized 37884.
Q. That tells us something. What's that?
A. It tells us that it bounced back and forth from tower to tower.
Q. Right.
A. Therefore, the phone is actually in a very smaller area, in that overlapped area.
Q. But, we don't know where?
A. I could not tell you where.
Q. We don't know who was using the phone, do we?
A. I do not know.
Q. We don't know what is said on the phone, do we? What was being said, do we know that?
A. Why are you yelling?
Q. I didn't know if you heard me or not.
A. I can hear you.
Q. We don't know what is being said, do we?
A. I have no idea, sir.
MR. SANTAGUIDA: Thank you.

THE COURT: Any other cross-examination?

MR. MOZENTER: No.

MR. GREY: No.

THE COURT: Any redirect?

MR. WZOREK: No, your Honor.

THE COURT: Thank you, Special Agent Shute.

(Witness leaves the witness stand)

I N D E X

	DIRECT	CROSS
WILLIAM SHUTE	3	25

C E R T I F I C A T E

SIDNEY S. ROTHSCHILD, being a United States Court Reporter, United States District Court, Eastern District of Pennsylvania, does hereby certify that he was authorized to and did report in shorthand, the above and foregoing proceedings, and that thereafter his shorthand notes were transcribed under his supervision, and that the foregoing pages contain a true and correct transcription of his shorthand notes taken therein.

Done and signed this 3rd day of March, 2008, in the City of Philadelphia, County of Philadelphia, State of Pennsylvania.

SIDNEY S. ROTHSCHILD

U.S. Court Reporters
United States District Court
Eastern District of Pennsylvania