

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

MBD-07-10192-RGS

IN RE APPLICATIONS OF THE UNITED STATES
OF AMERICA FOR ORDERS PURSUANT TO TITLE 18,
UNITED STATES CODE, SECTION 2703(d)

MEMORANDUM AND ORDER ON GOVERNMENT'S
MOTION FOR REQUEST FOR REVIEW

September 17, 2007

STEARNS, D.J.

INTRODUCTION

As part of an ongoing criminal investigation, the government sought a court order requiring certain cellular telephone companies to disclose a customer's cellular telephone records. In doing so, the government relied on provisions of the Stored Communications Act (SCA), 18 U.S.C. §§ 2701 *et seq.* The Magistrate Judge allowed the government access to the customer's subscriber information but refused it permission to access historical cell site information.¹ Subscriber information includes a customer's name and address, as well as telephone connection and billing records. Cell site information encompasses records identifying the relay tower or towers through which a customer's calls were handled. Magistrate Judge Alexander held that access to cell site information may be obtained only pursuant to a warrant issued on a showing of probable cause. She rejected the government's argument that it need show only "specific and articulable facts"

¹See In re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), ___ F. Supp. 2d ___, 2007 WL 2296406, at *4 (D. Mass. July 27, 2007) (In re Applications) (Alexander, U.S.M.J.).

demonstrating the relevance of the information to a criminal investigation (the standard set out in the SCA).² The case is before this court on the government's appeal of the Magistrate Judge's ruling.

BACKGROUND

Cellular telephone networks consist of a grouping of interconnected "cells." Each cell is serviced by a tower whose antennae transmit and receive signals from cellular telephones within a specific area of coverage. As a caller moves (or roams) through these areas, his or her phone is automatically switched to the tower that (at least in theory) provides the best reception. Cellular telephone companies maintain records of this switching information. The information is used, for among other business purposes, to assess roaming charges. However, the close proximity of cell towers in urban (and some suburban) areas has also imbued cell site information with a value to law enforcement: cell site information coupled with a basic knowledge of trigonometry makes it possible to identify with reasonable certainty the location from which a call was made.³

²The "specific and articulable facts" standard requires a showing of a particularized and objective basis for a suspicion of criminal activity. United States v. Cortez, 449 U.S. 411, 417-418 (1981). While the standards defining probable cause are "not readily, or even usefully, reduced to a neat set of legal rules," Illinois v. Gates, 462 U.S. 213, 232 (1983), probable cause requires facts sufficient to warrant a belief by a person of reasonable caution that the specific item(s) being sought constitute evidence of a crime. Texas v. Brown, 460 U.S. 730, 742 (1983) (plurality opinion).

³In urban areas, cell towers can be only hundreds of feet apart. In rural areas, towers are often ten miles or more apart. In re Application of United States for an Order for Disclosure of Telecomm. Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (S.D.N.Y. l).

The prospect that cell site information might be used as a surveillance tool has led to a disagreement among courts over the standard to be applied when the government requests access to prospective or “real time” cell site information, although a strong majority has opted for the probable cause standard.⁴ Here, however, the government does not seek prospective or real time information, but rather “historical cell site information . . . for the period May 1, 2007 to the date of the Court’s order”⁵ Government’s

⁴Decisions granting disclosure of prospective cell site information under the “specific and articulable” facts standard of the SCA include: 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); In re Application of the United States, 411 F. Supp. 2d 678 (W.D. La. 2006); In re Application of the United States for an Order for Prospective Cell Site Location Info., 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (S.D.N.Y. II); In re Application of the United States of America, 433 F.Supp.2d 804 (S.D. Tex. 2006); and S.D.N.Y. I. Decisions requiring a showing of probable cause under Fed. R. Crim. P. 41 include: In re Application of United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, ___ F. Supp. 2d ___, 2007 WL 2058924 (D.P.R. July 18, 2007) (D.P.R.); In re Application of United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Info., 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); In re Application of the United States of America, 441 F. Supp. 2d 816 (S.D. Tex. 2006); In re Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecomm. Records, 439 F. Supp. 2d 456 (D. Md. 2006); In re Application of the United States of America, 2006 WL 1876847 (N.D. Ind. July 5, 2006); In re Application of the United States of America, 416 F. Supp. 2d 390 (D. Md. 2006); In re Application of the United States of America, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) (W.D.N.Y.); In re Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134 (D.D.C. 2006); In re Applications of the U.S. for Orders Authorizing the Disclosure of Cell Site Info., 2005 WL 3658531 (D.D.C. Oct. 26, 2005); and In re an Application of U.S.A. for an Order (1) Authorizing the use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (E.D.N.Y.); In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (S.D. Tex I).

⁵Although no published opinion has directly addressed the issue, a number of courts have assumed or implied in *dicta* that disclosure of historical data is proper under the SCA’s specific and articulable facts standard. See D.P.R., 2007 WL 2058924, at *7 (“[T]he SCA, as its title announces, contemplates orders for *stored* rather than prospective

Application Pursuant to 18 U.S.C. § 2703(d) at 1. The issue squarely presented by this case of first impression is whether *historical* cell site information is obtainable (as the government argues) under section 2703(d) of the SCA.

DISCUSSION

Stored Communications Act

Section 2703(c) of the SCA addresses “[r]ecords concerning electronic communication service or remote computing service.” In relevant part, the Act provides that “a governmental entity 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)” by obtaining a court order pursuant to section 2703(d). Under this latter section, a court may issue a disclosure order provided that the government “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.”

information.”) (emphasis in original); S.D.N.Y. II, 460 F. Supp. 2d at 459 (“[T]he entire focus of the [SCA] is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service providers.”); W.D.N.Y., 415 F. Supp. 2d at 214 (“[T]he SCA authorizes the government to obtain *historical* cell site data, including location information”) (emphasis in original); S.D.N.Y. I, 405 F. Supp. 2d at 446-447 (noting the significant distinction between requests for “historical versus real time data” under the SCA); E.D.N.Y., 396 F. Supp. 2d at 303 n.6 (“If the government were seeking only historical cell site information, that would of course be correct (though of course in such circumstances there would be no issue to resolve, as § 2703(d) plainly allows such relief.”); S.D. Tex. I, 296 F. Supp. 2d at 759 n.16 (“[H]istorical cell site data more comfortably fits the category of transactional records covered by the SCA. Cell phone companies might legitimately compile such data for customized marketing and billing purposes.”).

The issue presented by this case is whether historical cell site information is obtainable under section 2703(d) of the SCA. To answer this question, the court must first determine whether section 2703(c)(1)(B) of the SCA applies.⁶ This requires a three-part inquiry. First, the court must determine whether the record holder is a “provider of electronic communication service,” defined by the SCA as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15).⁷ Cell phone service providers undisputedly fit within this definition.

Second, the court must determine whether historical cell site information is “a record or other information pertaining to a subscriber to or customer of” an electronic communications service. 18 U.S.C. § 2703(c)(1). Since neither the term “record” nor the term “information” is defined by the SCA, a court must look to the meaning of the terms in their ordinary usage. In the relevant context, a record means something stored or archived. The term information is synonymous with data. Cell phone service providers store data gleaned from the cell towers through which telephone calls are routed. Thus, historical cell site information is a “record or other information pertaining to” a customer, as it contains data specific to the handling of a customer’s call.⁸

⁶Section 2703(c)(1)(B) authorizes the disclosure of records or other information pursuant to a court order issued under section 2703(d).

⁷Definitions of the terms used in the SCA are set out in 18 U.S.C. § 2510. See 18 U.S.C. § 2711(1).

⁸The Magistrate Judge was of the view that this reading “glosses over a critical distinction between historical cell site information and records or other information.” In re Applications, 2007 WL 2296406, at *4. Magistrate Judge Alexander reasoned that because “historical records provide relatively sterile data . . . while historical cell site information provides the location of a person or object,” historical cell site information is

Finally, the court must determine whether historical cell site information is “content” information, which is defined by the SCA as “any information concerning the substance, purport, or meaning of [a] communication.” 18 U.S.C. § 2510(8). The location of a cell tower in relation to the point of origin (or termination) of a call discloses nothing about the substance of the call itself. It is therefore “noncontent” information. Because historical cell site information clearly satisfies each of the three definitional requirements of section 2703(c), a section 2703(d) order requiring the disclosure of historical cell site information may issue on a showing of “specific and articulable facts” and no more.⁹ The government’s sealed application in this case, which this court has reviewed *in camera*, meets that standard.

Fourth Amendment

tantamount to information provided by a “tracking device.” See 18 U.S.C. § 3117(b). *Id.* I disagree with this analogy for two reasons. First, section 2703(c) makes a clear distinction between “sterile” subscriber data and more detailed noncontent transactional data. Under section 2703(c)(2), the government may obtain basic subscriber records, such as name, address, length of service, and means of payment (including any credit card or bank account number), by mere subpoena. Thus, the “records and other information” obtainable by means of a section 2703(d) order must consist of data containing greater detail than the records subject to an administrative subpoena by section 2703(c)(2). Any other construction would render section 2703(c)(2) superfluous. Second, nothing in the 18 U.S.C. § 3117(b) definition of a mobile tracking device places a limitation on the “records or other information” obtainable pursuant to a section 2703(d) order. See *S.D.N.Y. I*, 405 F. Supp. 2d at 445-446.

⁹ “[W]hen a statute speaks with clarity to an issue[,] judicial inquiry into the statute’s meaning, in all but the most extraordinary circumstances, is finished.” Estate of Cowart v. Nicklos Drilling Co., 505 U.S. 469, 475 (1992). “[C]ourts must presume that a legislature says in a statute what it means and means in a statute what it says.” Barnhart v. Sigmon Coal Co., 534 U.S. 438, 461-462 (2002).

The issue remains, however, whether the Fourth Amendment's probable cause requirement nonetheless preempts the more relaxed provisions of the SCA governing the disclosure of historical cell site information. What concerned the Magistrate Judge was a scenario in which the government utilized access to forward-looking or real time cell site information to physically track a cell phone user. In this circumstance, the Magistrate Judge could see "no reason to treat cell phone tracking any different than other forms of tracking which routinely require probable cause." In re Applications, 2007 WL 2296406, at *9 (internal citations and quotations omitted). Whether the government has access to the technology (one would think it does), or the physical resources (it might not in the ordinary case) to contemporaneously monitor the switching of cellular telephone calls is an interesting question, but one that is not raised by this case.¹⁰ Here the government seeks only historical information that it hopes will reveal where a subject of interest happened to be at a given time in the past. This information will not, however, tell the government anything about the subject's location at the present (or for that matter, his or her location at any given time in the future).

A second consideration (the issue that concerned the Magistrate Judge, although not raised by the facts of this case) is this: even if an order requiring the disclosure of prospective cell site information allowed the government to "track" a suspect (or more accurately his or her phone) into a protected area like a home, would any reasonable Fourth Amendment expectation of privacy be compromised as a result? Unlike United

¹⁰As observed earlier, in this scenario most courts have required a showing of probable cause as a predicate to disclosure.

States v. Karo, 468 U.S. 705, 715 (1984), where the electronic beeper concealed in the drum of ether disclosed not only the location of defendant's home, but also the fact that criminal activity was afoot (which featured prominently in the search warrant affidavit), there is nothing presumptively illegal about the possession of a cellular phone. The most that the "tracked" cell phone might reveal is that its owner might presently be found in the home (assuming that the phone had not been loaned to someone else). There is nothing, however, about that disclosure that is any more incriminating or revealing than what could be gleaned from the activation of a pen register or from physical surveillance. Moreover, outside of the home it is doubtful that the tracking of a cell phone has any Fourth Amendment implication whatsoever. See Karo, 468 U.S. at 713-720 (distinguishing the unlawful warrantless monitoring of beeper signals that disclose information about a private dwelling from information that could be obtained from public observation); United States v. Knotts, 460 U.S. 276, 282 (1983) (no warrant is required when law enforcement monitors the signals of a concealed beeper transported along a public highway); cf. Smith v. Maryland, 442 U.S. 735, 744-745 (1979) (a phone subscriber has no reasonable expectation of privacy in the numbers he or she dials through telephone company switching equipment).

Finally, any speculation about improper government "tracking" is premature. Fourth Amendment questions are difficult to resolve in the abstract. Assuming – as the Magistrate Judge warned – that prospective or real time cell site information is capable of

transforming a cellular telephone into a “tracking device,”¹¹ it should be left to an aggrieved defendant to litigate the constitutionality of warrantless law enforcement surveillance by means of such a “device” in the more appropriate context of a motion to suppress.

ORDER

For the foregoing reasons, the decision of the Magistrate Judge is REVERSED. The government’s application for an order directing certain cellular telephone companies to disclose historical cell site information is GRANTED.

SO ORDERED.

/s/ Richard G. Stearns

UNITED STATES DISTRICT JUDGE

¹¹I am not, however, persuaded of the relevance of the mobile device tracking statute, 18 U.S.C. § 3117, to the issue. The statute governs the “installation” of tracking devices. The “tracking” of a cell phone does not require the installation of any sort of device. The telephone does the job by itself.

Publisher Information

**Note* This page is not part of the opinion as entered by the court.
The docket information provided on this page is for the benefit
of publishers of these opinions.**

1:07-mc-10192-RGS *SEALED* In Re: Applications for Orders (Appeal of Magistrate Judge Decision)
Richard G. Stearns, presiding
Date filed: 08/02/2007
Date terminated: 09/17/2007 Date of last filing: 09/17/2007

Attorneys

Stephen P. Heymann United States Attorney's Office John Joseph Moakley Federal Courthouse 1 Courthouse Way Suite 9200 Boston, MA 02210 617-748-3100 Stephen.Heymann@usdoj.gov Assigned: 08/02/2007 LEAD ATTORNEY ATTORNEY TO BE NOTICED	representing	United States of America (Petitioner)
Robert E. Richardson United States Attorney's Office Suite 9200 1 Courthouse Way Boston, MA 02210 617-748-3247 617-748-3951 (fax) robert.richardson@usdoj.gov Assigned: 08/02/2007 LEAD ATTORNEY ATTORNEY TO BE NOTICED	representing	United States of America (Petitioner)