IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF A PEN REGISTER AND A CALLER IDENTIFICATION SYSTEM ON TELEPHONE NUMBERS [sealed] AND [sealed] AND THE PRODUCTION OF REAL TIME CELL SITE INFORMATION.	*	No. 05-4486 JKB

*****

MEMORANDUM OPINION

On the evening of November 3, 2005, in furtherance of a criminal investigation, the government sought an order from this court authorizing the installation and use of a pen register and caller identification/ caller identification deluxe system with respect to a suspect's cellular telephone. The government also requested an order directing the relevant wireless communications service provider to disclose "real time cell site information," which would reveal the physical location of the person in possession of the cell phone whenever the phone was on. The government did not seek information regarding the contents of any communication.

After reviewing the government's application, including proffered "specific and articulable facts showing . . . reasonable grounds to believe that . . . the records or other information sought [would be] relevant and material to an ongoing criminal investigation," 18 U.S.C. 2703(d), and after reviewing the statutes referenced in the application, the court concluded the cited authority and the proffer were insufficient to support the government's request. The court determined the government needed to show probable cause in a sworn

affidavit in order to obtain real time cell site information.[1] Subsequently the government submitted a letter, which has been docketed (Paper No. 3), outlining its position that an order to obtain "prospective" cell site information can be entered upon less than probable cause pursuant to a combination of statutes.[2]

The issue presented by this application is whether existing statutes allow the government to obtain real time cell site information upon a showing of less than probable cause. For the reasons stated below, the court determines that the statutes cited by the government do not allow access to such information, and the court is left with only its general authority to issue a Rule 41 warrant upon a showing of probable cause. *See* Fed. R. Crim. P. 41. As Rule 41 comports with the Fourth Amendment to the United States Constitution, the court need not reach the constitutional issues the government's application otherwise would implicate.

At least two other courts have addressed this issue in depth. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 2005 WL 2656621 (S.D. Tex. Oct. 14, 2005) (Smith, M.J.) ("*Cell Site Location Authority*"); *In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site*

---

[1]After the court denied its application, the government immediately provided a sworn affidavit establishing probable cause and the court issued the requested order. I write now to explain the initial denial.

[2]The government appears to use the terms "real time cell site information" and "prospective cell site information" interchangeably, but the two are distinct. *See infra* Part I. The government asked for "real time cell site information" in its initial application, so this opinion is limited to real time cell site information. Where I describe arguments made in the government's docketed letter, which discusses "prospective cell site information," I substitute "real time" for "prospective."

Information, 2005 WL 2739208 (E.D.N.Y. Oct. 24, 2005) (Orenstein, M.J.) ("*Cell Site Information*"). After independent consideration, this court reached the same conclusion as Judges Smith and Orenstein and will briefly explain its reasoning by borrowing liberally from their extensive opinions.

I. Background[3]

When powered on, a cellular telephone automatically communicates with one or more cell sites, also known as "cell towers." The phone constantly seeks the cell site that provides the best reception, re-scanning for cell sites every seven seconds or when the signal strength weakens, regardless of whether a call is made. As the phone changes location, it automatically switches to the cell site that provides the best reception. Wireless service providers typically keep track of the identity of the cell towers serving a phone at any point in time and the aspect of each tower facing the phone. When a phone is in touch with more than one tower, the service provider (or law enforcement, if given permission) can compare the signals and locate the phone through a process of triangulation.

The government contends that "at best" cell site information can provide a cell phone's "general location within a broad area surrounding a particular cell-site tower." (Paper No. 3 at 8.) In fact, cell site information can provide much more precise location data. In 1997, the Federal Communications Commission ("FCC") issued "Enhanced 911" rules requiring wireless service providers to identify more precisely the location of users making 911 calls. In order to comply, some providers chose to install global positioning chips while others chose to use cell

[3]*See generally Cell Site Location Authority*, 2005 WL 2656621, at *2-*3; Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J. L. & Tech. 307, 308-09 (2004).

site information. Under FCC mandate, by the end of 2005 those providers choosing cell site information must be able to pinpoint 67 percent of calls within 100 meters and 95 percent of calls within 300 meters. *See* 47 C.F.R. § 20.18(h)(1). As the technology develops and more cell phone towers are built, the accuracy will only improve.[4]

"Real time" cell site information refers to data used by the government to identify the location of a phone at the present moment. Real time cell site information is a subset of "prospective" cell site information, which refers to all cell site information that is generated after the government has received court permission to acquire it.[5] Records stored by the wireless service provider that detail the location of a cell phone in the past (i.e.: prior to entry of the court order authorizing government acquisition) are known as "historical" cell site information.

The use of real time cell site information by law enforcement for tracking purposes is a relatively new phenomenon and Congress has yet to legislate on the specific subject. As such, the court must analyze disclosure of real time cell site information under the existing statutory scheme. Electronic surveillance law is largely governed by the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986). *See generally Cell Site Location Authority*, 2005 WL 2656621, at *3-*4. Although the ECPA does not specifically

---

[4]The accuracy of triangulation increases as a cell phone communicates with more towers. Thus, in urban areas the density of towers gives providers more accurate location information than in a rural area where there may be a single tower covering several hundred square miles. *See* Note, *supra* note 2, at 309-310.

[5]For example, imagine the government receives a court order on a Monday granting access to prospective cell site information (i.e. all cell site information generated going forward). On Thursday, the government begins tracking the phone in real time; such information is both prospective and real time cell site information. On Friday, the government goes back and accesses the records of the phone's location on Tuesday and Wednesday; such information is prospective but not real time cell site information.

articulate the legal process required for the government to collect real time cell site information, the law does contain provisions governing stored electronic information, pen register and trap and trace devices, and tracking devices. The court must determine which, if any, of these provisions apply.

II. The Government's "Hybrid" Theory

The government argues that real time cell site information may be disclosed pursuant to the combined authority of 18 U.S.C. § 3121 *et seq.* (the "Pen/Trap Statute") and 18 U.S.C. § 2701 *et seq.* (the "Stored Communications Act" or "SCA") provided the government offers "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." (Paper No. 3 at 2, citing 18 U.S.C. § 2703(d).) More specifically, the government contends that the SCA authorizes disclosure of historical cell site information and, when combined with the Pen/Trap Statute, also authorizes disclosure of real time cell site information. Judges Smith and Orenstein reject this "hybrid theory" under almost identical rationales. *See Cell Site Location Authority*, 2005 WL 2656621, at *12-*16; *Cell Site Information*, 2005 WL 2739208, at *23-*26. This court joins them.

A. The Stored Communications Act

Title II of the ECPA created a new chapter of the criminal code dealing with access to stored communications and transaction records, which is known as the "Stored Communications Act," codified at 18 U.S.C. § 2701 *et seq*. The SCA authorizes the government to require disclosure of stored communications and transaction records by third party service providers. Sections 2703(a) and (b) grant the government access to the contents of wire or electronic

communications and generally require either notice to the customer or a search warrant under Rule 41 or the equivalent state provision. Cell site information does not qualify as "the contents of a communication" within the meaning of 18 U.S.C. § 2703(a) and (b) because it conveys data concerning the location of a cell phone and its possessor[6] rather than the contents of any phone conversation.

The government contends that cell site information falls under Section 2703(c), which grants the government access to "a record or other information pertaining to a subscriber to or a customer of such service (not including the contents of a communication)." 18 U.S.C. § 2703(c). The government may obtain non-content information as defined in Section 2703(c) through a court order if it "offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

The SCA does not define the term "record or other information pertaining to a subscriber to or a customer of such service." The 1986 Senate Report only notes that "[t]he information involved is information about the customer's use of the service." S. Rep. No. 99-541, at 38 (1986). In its original form, the SCA permitted disclosure of non-content information by subpoena or court order. In 1994, Congress amended the SCA by passing the Communications

[6]I use the term "possessor" rather than "user" because cell site information allows tracking of a cell phone regardless of whether the phone is in "use." If the phone is turned on, the wireless service provider or the government may track the movement of the possessor of the phone even if he makes no outgoing calls or receives no incoming calls. The government may engage in "pinging," in which a government agent calls the target cell phone repeatedly without letting the phone ring, in order to collect the cell site information. *See United States v. Forest*, 355 F.3d 942, 947 (6th Cir. 2004) (DEA agent "pinged" suspected cocaine trafficker's cell phone several times in one day in order to track the suspect's movement).

Assistance for Law Enforcement Act (CALEA), P.L. 103-313, 108 Sta. 4279 (1004). After the amendments, basic subscriber information (e.g. name, address, duration of calls) could still be obtained by subpoena but disclosure of all other non-content information (the "record or other information pertaining to a subscriber" in Section 2703(c)) required at least a court order. According to the government, the fact that Congress did not entirely eliminate access to this more detailed non-content information in 1994 demonstrates Congress intended to authorize courts to order the disclosure of a broad array of non-content information, such as cell site information, pursuant to Section 2703(c).

The government also points to the legislative record behind the CALEA as evidence Section 2703(c) applies to cell site information. *See* H.R. Rep. No. 103-827(I), at 31 (1994) ("House CALEA Report"). In discussing the changes to Section 2703(c), the House CALEA Report addressed "transactional records from on-line communications services" and acknowledged that they would reveal more than telephone records or mail records. *Id.* According to the government, Congress intended the amendments to authorize disclosure of e-mail addresses used in correspondence, which implicate a higher privacy interest than cell site information. In other words, if the government has access to the former, it must have access to the latter.

The court is not persuaded by the government's argument. *Historical* cell site information may be covered by 18 U.S.C. § 2703(c), but such information is not at issue here.[7] To the extent the government claims to use the combined authority of the SCA and the Pen/Trap

[7]Some might argue that historical cell site information detailing the location of a phone and its possessor in an area not open to the public implicates the Fourth Amendment and cannot be disclosed absent a showing of probable cause. I need not address this issue here.

Statute, the government must demonstrate that the SCA authorizes the acquisition of *real time* cell site information, a burden it has not met. The 1994 amendments to the SCA raised, rather than lowered, the standard for acquiring access to non-content information. The court will not draw an inference from these amendments that Congress intended to expand the reach of the SCA to real time cell site information. Furthermore, the government's reference to the legislative record reveals the amendments concerned e-mail information, not cell site information, and especially not *real time* cell site information. Finally, the court is not convinced an individual's privacy interest in the addresses of his e-mail correspondents exceeds his privacy interest in his real-time location.[8]

Judge Smith provides two additional arguments against allowing access to real time cell site information under Section 2703(c) and (d). *See Cell Site Location Authority*, 2005 WL 2656621, *10-*12. First, the section applies to "[r]ecords concerning electronic communication service or remote computing service." 18 U.S.C. § 2703(c). The term "remote computing service" pertains to e-mail and does not implicate cell site information. The term "electronic communication service" is defined elsewhere in the ECPA as "any service which provides to users thereof the ability to send or receive *wire or electronic communications*." 18 U.S.C. §§ 2510(15), 2711(1) (emphasis added). The acquisition of real time cell site information does not

[8]Although I need not decide the issue here, an e-mail address may be analogous to a dialed phone number, which implicates no privacy interest under the 4th Amendment. *See Smith v. Maryland*, 442 U.S. 735 (1979) (holding that telephone users had no subjective expectations of privacy in dialed telephone numbers and any such expectation was not one society was prepared to recognize). In comparison, an individual's location in a non-public place undoubtedly implicates the 4th Amendment. *See United States v. Karo*, 468 U.S. 705, 714 (1984) ("private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable").

involve the transfer of "wire or electronic communications" as those terms are defined. "Electronic communication" excludes "any communication from a tracking device," 18 U.S.C. § 2510(12)(C), and as discussed later the acquisition of real time cell site information converts a cell phone into a tracking device under 18 U.S.C. § 3117. "Wire communication" excludes communication not involving the human voice, and the transmission of cell site information does not involve the transfer of the human voice. 18 U.S.C. §§ 2510(1), (18). In sum, cell site information is not a record concerning electronic communication service or remote computing service and therefore is not covered by Section 2703(c).

Second, the structural differences between the SCA and the electronic surveillance statutes suggest Congress did not intend the SCA to allow real time tracking of a cell phone possessor. Unlike the parts of the ECPA regulating real-time surveillance, the SCA regulates access to records and communications in storage. As such, the SCA imposes no limit on the duration of the government's access, no provision for renewal of the court order, no requirement for periodic reports to the court by the government, and no automatic sealing of court records. In contrast, all of these provisions appear in statutes governing prospective surveillance like wiretap and pen/trap orders. The distinction shows the SCA was not meant to govern this new form of tracking through the use of real time cell site information.

B. The Pen/Trap Statute

Recognizing the SCA refers to "stored" communications, the government does not claim 18 U.S.C. 2703(c) alone authorizes disclosure of *real time* cell site information. Instead, the government turns to the Pen/Trap Statute in Title III of the ECPA, which pertains to pen registers and trap/trace devices. *See* 18 U.S.C. §§ 3121-3127, Paper No. 3 at 4. A pen register

records telephone numbers dialed for outgoing calls from the target phone and a trap/trace device (sometimes called a "caller identification system") records the telephone numbers of those calling the target phone. In order to obtain authorization for installation of a pen register and trap/trace device, the government need only certify that information likely to be obtained by the devices is "relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2). The government contends the USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("PATRIOT Act") expanded the definition of "pen register" and "trap and trace device" to include real time cell site information.

The government may not seek cell site information pursuant to the Pen/Trap Statute, however, because the CALEA explicitly forbids service providers from disclosing "any information that may disclose the physical location of the subscriber" when the government proceeds "solely pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2). The government reads the CALEA as affirmatively authorizing access to information disclosing the physical location of the subscriber so long as the government does not act "solely pursuant" to the Pen/Trap Statute. Here, the government contends it proceeds not only under the Pen/Trap Statute but also under Section 2703(c) and (d) of the SCA. The problem with this is that the government *cannot* act pursuant to these provisions of the SCA because they do not authorize the disclosure of *real time* cell site information.[9] *See* discussion *supra* Part II.A.

Judge Orenstein concisely summarizes the many other problems with the hybrid theory in

[9]In fact, the government seems to recognize this because it argues only that the SCA authorizes disclosure of *historical* cell site information.

italicized headings in his opinion, and they will not be recounted here. *See Cell Site Information*, 2005 WL 2739208, at *23-*25. The theory hinges on several doubtful propositions, such as the contention that the PATRIOT Act modified the Pen/Trap statute so it now encompasses real time cell site information. Perhaps more importantly, the statutory provisions relied on by the government were passed by different Congresses at various times over a 15-year period and barely reference one another. Judge Smith aptly notes:

> The sum of these questionable premises is no greater than its defective parts. The most glaring difficulty in meshing these disparate statutory provisions is that with a single exception they do not cross-reference one another. The Pen/Trap Statute does not mention the SCA or CALEA; SCA § 2703 does not mention CALEA or the Pen/Trap Statute; and the CALEA proviso does not mention the SCA. CALEA does refer to the Pen/Trap Statute, but only in the negative sense of disclaiming its applicability. Surely if these various statutory provisions were intended to give birth to a new breed of electronic surveillance, one would expect Congress to have openly acknowledged paternity somewhere along the way. This is especially so given that no other form of electronic surveillance has the mixed statutory parentage that prospective cell site data is claimed to have.

Cell Site Location Authority, 2005 WL 2656621, at *15.

III. Real Time Cell Site Information as a Tracking Device

Although disclosure of real time cell site information is not authorized by the SCA or the Pen/Trap Statute, this court may look to another provision of the ECPA. Real time cell site information, when used to monitor the location and movement of a cell phone and its possessor over time, is governed by the ECPA's section on "tracking devices."

Title I of the ECPA defines the term "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). The government argues that cell-site data does not actually "permit the tracking of the movement of a person or object" because it is too imprecise. The definition of "tracking device" is broad,

however, and contains no articulation of how precise a device must be. Moreover, cell-site data unquestionably permits the tracking of the movement of a cell phone when two-thirds of users can be pinpointed within 100 meters and 95 percent within 300 meters. One example of the technique is described in the opinion deciding *Forest*:

> In order to reestablish visual contact, a DEA agent dialed Garner's cellular phone (without allowing it to ring) several times that day and used Sprint's computer data to determine which transmission towers were being "hit" by Garner's phone. This "cell-site data" revealed the general location of Garner. From this data, DEA agents determined that Garner had traveled to the Cleveland area and then returned to the area of Youngstown/Warren.

355 F.3d at 947.

The government argues Congress intended "tracking devices" to mean homing devices that are separate and apart from cell phones, as evidenced by language in the Senate Report on the ECPA. First, as Judge Smith notes, this definition never made it into the United States Code. *Cell Site Location Authority*, 2005 WL 2656621, at *5. Second, the traditional homing devices to which the government refers are now monitored via radio signals using the same cell phone towers used to transmit cell site data. *Id.* at *6. "Given this convergence in technology, the distinction between cell site data and information gathered by a tracking device has practically vanished." *Id.*

Unlike other provisions in the ECPA, 18 U.S.C. § 3117 articulates no standard for obtaining permission to install and monitor a tracking device. The only limit on such devices is the Fourth Amendment. The warrantless monitoring of a tracking device located in a public place generally does not implicate the Fourth Amendment. *See United States v. Knotts*, 460 U.S. 276, 285 (1983) (warrantless monitoring of an electronic tracking device inside a container of chemicals did not violate the Fourth Amendment when it revealed no information that could not

have been obtained through visual surveillance); *Karo*, 468 U.S. at 721 (there is no reasonable expectation of privacy when a tracking device is monitored as it travels through a public place). However, warrantless monitoring of an electronic tracking device in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence. *Karo*, 468 U.S. at 715.

If acquisition of real time cell site information is equivalent to a tracking device, it would seem the government is not constitutionally required to obtain a warrant provided the phone remains in a public place where visual surveillance would be available. But, unlike cases in which the government itself installs an electronic tracking device in a public place (typically on a vehicle parked on a public street) and then monitors it, here the government presumably *needs* some sort of court order, without which it cannot compel the wireless service provider to furnish the cell site information.[10] The government approached this court seeking such an order, and since the statutes it proffers are insufficient to authorize one, the only other authority available to the court is Rule 41.[11] *See Cell Site Information*, 2005 WL 2739208, at *26 ("to the extent the

[10]Furthermore, the government cannot guarantee the cell phone and its possessor will remain in a public place. "The mere possibility of such an invasion [of privacy] is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant." *Cell Site Location Authority*, 2005 WL 2656621, at *9.

[11] Up to this point, the court has addressed only the standard for real time cell site information, but the court's reasoning probably applies to all prospective cell site information, not just that accessed in real time. *See supra* Part I and note 5. The authority proffered by the government appears insufficient to allow disclosure of any prospective cell site information, for mostly the same reasons the proffered authority was insufficient to allow disclosure of real time cell site information. Section 2703(c) of the SCA does not seem to contemplate allowing the government to access any cell site information that does not exist at the time the order is entered. If it did, the provision would include temporal limitations and renewal requirements like other statutes governing prospective surveillance.

government seeks a judicial imprimatur for its acquisition in real time of prospective cell site information, it must proceed under Rule 41"). Rule 41 permits the court to issue a warrant to search for evidence of a crime upon a showing of probable cause. Fed. R. Crim. P. 41(d)(1).

In light of this ruling, the procedure in this court is as follows: When the government seeks to acquire and use real time cell site information to identify the location and movement of a phone and its possessor in real time, the court will issue a warrant upon a sworn affidavit demonstrating probable cause to believe the information will yield evidence of a crime. The court will not enter an order authorizing disclosure of real time cell site information under authority other than Rule 41, nor upon a showing of less than probable cause. To the extent the government seeks to act without a warrant, the government acts at its peril, as it may not monitor an electronic tracking device in a private place without a warrant.[12] *Karo*, 468 U.S. at 715.

---

[12]Like Judges Smith and Orenstein, I need not decide whether the government may obtain cell site information without permission from the court. *See Cell Site Location Authority*, 2005 WL 2656621, at *9 ("For purposes of this decision it is unnecessary to draw the line between permissible and impermissible warrantless monitoring of cell site data. As in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights."); *Cell Site Information*, 2005 WL 2739208, at *26 ("to the extent the government asserts that it can proceed without a warrant, on the ground that no cognizable privacy interest is at stake (a position upon which it can, as a practical matter, act at its own risk), I make no decision"). In this case, the government sought my permission and I required it to show probable cause.

The government claims a warrant is never required because cell site information does not implicate the Fourth Amendment, even when the possessor resides in a private place. The government reaches this conclusion by analogizing cell site information to dialed telephone numbers. *See Smith*, 442 U.S. at 742-44 (dialed telephone numbers do not implicate the Fourth Amendment). The Sixth Circuit and Judge Smith rejected this analogy, and I join them. *Forest*, 355 F.3d at 951; *Cell Site Location Authority*, 2005 WL 2656621, at *8. Cell site information is not affirmatively and actively conveyed by the phone's possessor; the cell phone transmits the information automatically without the possessor's awareness and possibly without his knowledge. Further, the cell phone can be "pinged" without the possessor's awareness or knowledge.

(continued...)

November 28, 2005 /s/

Date James K. Bredar
United States Magistrate Judge

[12](...continued)

The Fourth Amendment applies when (1) an individual has "exhibited an actual (subjective) expectation of privacy" and (2) the individual's subjective expectation of privacy is "one that society is prepared to recognize as reasonable." *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Contrary to the government's suggestion, I do not believe most cell phone possessors realize they can be located within 100-300 meters any time their phone is turned on. Moreover, cell phone possessors' expectation of privacy, at least when they are in a non-public place, seems altogether reasonable. Those who choose to carry a cell phone, which has been turned on, cannot reasonably be deemed to have consented to the tracking of their movement by the government.