Congressional Research Service

MEMORANDUM June 29, 2010

To: Senate Intelligence Committee
Attention: John Dickas

From: Gina Stevens, Legislative Attorney, x7-2581
Alison M. Smith, Legislative Attorney, x7-6054
Jordan Segall, Law Clerk, x7-5123

Subject: **Legal Standard for Disclosure of Cell-Site Information (CSI) and Geolocation Information**

This memorandum[1] was prepared to respond to your request for a legal overview of cases concerning government requests for geolocation information held by private companies to find a customer's location, and for a discussion of the scope and conflicting nature of those cases. Geolocation information "can give the location of a cell phone within several hundred meters."[2] Cell-site information (CSI) generally "provides the location of the cell phone tower supplying service to a cell phone when it is actually engaged in a call."[3] You have inquired as to what legal standard is necessary to obtain court ordered disclosure of cell-site information and geolocation information from cell phone service providers. Most of the cases discussed below involve government applications to obtain cell-site location information.

As noted by scholars, advances in cellular phone technology "are occurring so rapidly that they blur distinctions made by legislatures and courts as to what is required to investigate, track, and/or search and seize a cellular telephone."[4] Reform proponents contend that "ECPA [Electronic Communications Privacy

---

[1] *See* CRS Report 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, by Gina Stevens and Charles Doyle for further information on this topic.

[2] In the Matter of the Application of the United States for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone Number ESN, 2006 WL 6217584 (D.D.C. 2006). " 'Real time' cell site information refers to data used by the government to identify . . . the location of a phone at the present moment . . . 'prospective' cell site information . . . refers to all cell site information that is generated after the government has received court permission to acquire . . . 'historical' cell site information . . . constitutes the records stored by a wireless service provider that detail the location of a cell phone in the past." Deborah F. Buckman, *Allowable Uses of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 ALR Fed. 2d 537, 545 (2010).

[3] *Id.*

[4] Clifford S. Fishman and Ann T. McKenna, *Wiretapping and Eavesdropping: Surveillance in the Internet Age* § 28.2 (3d ed. 2008).

Act] is a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty for both service providers and law enforcement agencies."[5]

Background

In the area of electronic surveillance law, there are four broad categories of surveillance, each with its own standard for obtaining court ordered disclosure or monitoring. Those categories are: (1) wiretaps, which are authorized pursuant to 18 U.S.C. §§ 2510-2522, upon what could be called a "probable cause plus" showing; (2) tracking devices, which are authorized pursuant to 18 U.S.C. § 3117, upon a Rule 41 probable cause showing;[6] (3) stored communications and subscriber records, which are authorized pursuant to the Stored Communication Act (SCA) upon a showing of specific and articulable facts showing that there are reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation;[7]and (4) pen registers and trap and trace devices authorized pursuant to the pen register statute (PRS),[8] upon the government's certification that the information sought is relevant and material to an ongoing criminal investigation.[9] Congress amended the SCA by passing the Communications Assistance for Law Enforcement Act of 1994 (CALEA).[10]

In criminal prosecutions, the Department of Justice (DOJ) has requested the "disclosure of the location of cell site/sector (physical address)"[11] information at points of call origination, termination, and during the

---

[5] Digital Due Process Coalition, *Modernizing Surveillance Laws for the Internet Age, available at* http://www.digitalddueprocess.org/index.cfm?objectid=DF652CE0-2552-11DF-B455000C296BA163.

[6] Rule 41 provides that the government may secure a warrant upon a showing of probable cause. A judge must issue the warrant after receiving an affidavit from a law enforcement officer if there is probable cause to search for and seize a person or property or to install and use a tracking device. Fed. R. Crim. P. 41. A tracking device is defined in 18 U.S.C. § 31117 (2006) as "an electronic or mechanical device which permits the tracking of the movement of a person or object."

[7] The Stored Communications Act (SCA), codified at 18 U.S.C. §§2701-2712 (2006), prohibits a provider of an electronic communication service or remote computing service from disclosing the contents of, or a record or other information pertinent to, a customer or subscriber to the government, except as otherwise authorized. Electronic communications excludes any communication from a tracking device, as defined in 18 U.S.C. § 3117 (2006), "an electronic or mechanical device which permits the tracking of the movement of a person or object." The exceptions to the governmental prohibition are when the government has: (1) obtained a warrant under the Federal Rules of Criminal Procedure, (2) obtained a court order under § 2703(d), (3) obtained subscriber consent to disclosure, (4) submitted a written request relevant to an investigation of telemarketing fraud, or (5) sought basic account information.

[8] The pen register statute, codified at 18 U.S.C.S. § 3121 et seq. (2006), requires that, absent emergency, the government must obtain a court order prior to installing or using a Trap and Trace, it may do so merely upon certification that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency. 18 U.S.C.S. § 3122(b)(2) (2006). Such orders routinely authorize real-time electronic monitoring of telephone call information for a limited duration, typically sixty (60) days. 18 U.S.C.S. § 3123(c) (2006).

[9] *See In re* Application of the United States of America for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F.Supp.2d 747, 753 (S.D.Tex.2005) (hereinafter "Smith Opinion").

[10] CALEA requires telecommunications carriers to acquire and implement technology to isolate and provide, on appropriate lawful authority, intercepted content and call-identifying information. Telecommunications carriers must provide access to call-identifying information before, during, or immediately after the transmission of a wire or electronic communication. Information acquired solely pursuant to the authority for pen registers and trap and trace devices may not yield information that discloses the physical location of the subscriber, except to the extent that the location may be determined from the telephone number. *See* 47 U.S.C. §§ 1001 *et seq.* (2006).

[11] 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 Information, 384 F. Supp. 2d 562, 563 (E.D.N.Y. 2005) (hereinafter "Orenstein Opinion I").

progress of the call. This information is stored by cellular telephone companies when the cellular telephone is operational through the phone's roaming antenna function, which allows the phone to link with the closest cell phone tower for the service provider. The information catalogs these changes in tower connection and also is cataloged in the context of individual telephone calls, showing the closest tower at the beginning of the telephone call and the closest tower at the end of the call. This information is limited, however, because towers can be up to 10 or more miles apart, and the location is not pinpointed since there is no GPS information involved. Records also do not indicate a phone's distance from the serving tower. The information can, however, provide a general indication of where a cell phone call was made, and the location can be pin-pointed more specifically through a process known as triangulation in which the angles of the various signals are calculated when two cell towers are involved.[12] In 2005, the FCC mandated that cell phones be capable of being located within 100 meters for public safety purposes.[13]

Legal Overview of Cases

Federal district courts are divided on the proper statutory authority and procedural requirements for government access to CSI and geolocation information.[14] Several magistrates have thoroughly examined the government applications for CSI.[15] For example, a court in the Western District of Pennsylvania rejected the government's application, and affirmed the magistrate's order requiring a warrant based on probable cause under the Fourth Amendment.[16] The Third Circuit Court of Appeals heard oral arguments in February and is preparing to rule on an appeal denying the government's application for cell-site location information, based on the SCA alone or in tandem with the pen register statute.

---

[12] *See* "Smith Opinion I," 396 F. Supp. 2d 747.

[13] In the Wireless Communication and Public Safety Act, P.L. 106-81, a nationwide emergency service for cell phone users was mandated with Congress recognizing the privacy interest of one's physical location. As such, in authorizing disclosure of specifically limited location information for emergency services they disallowed access to location information unless expressly authorized. 47 U.S.C. § 222(f). Location information provided to 911 operators is comprised of GPS data, triangulation data, and single cell site data. *See generally* Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L. J. 381, 384-88 (2003).

[14] *Compare In re* Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F.Supp.2d 947 (E.D. Wis. 2006) to In re Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (hereinafter "Gorenstein Opinion").

[15] It is to be noted that there have been numerous decisions discussing the issue of cell-site information, particularly at the Magistrate level where the issue has been painstakingly analyzed. Attempting to represent all cases could constitute a treatise. *See* Ian James Samuel, *Warrantless Location Tracking*, 83 N.Y.U. L. REV. 1324, n.9 (2008).

[16] 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, 534 F. Supp. 2d 585 (W.D. Pa. 2008). The principal object of the Fourth Amendment is the protection of privacy and people rather than property and places. In *Katz v. United States*, 389 U.S. 347-353 (1967), the Court stated that "[T]he test propounded . . . is whether there is an expectation of privacy upon which one may "justifiably" rely." That is, the capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was reasonable expectation of freedom from governmental intrusion. This reasonable expectation must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law, or to understandings that are recognized and permitted by society. Rakas v. Illinois, 439 U.S. 128 (1978). When the Fourth Amendment protects information it does so with a probable cause standard and particularity backed by the exclusionary rule.

It does not appear that another court has ruled in such a manner, requiring a warrant under the Fourth Amendment based upon a showing of probable cause for government access to cellular-telephone-derived location information, historic or prospective. Many courts have rejected Fourth Amendment challenges based on the fact that (1) the information tells nothing about the subject's location in the present when it is historical cell-site information, (2) the information does not reveal a particular location unless involving multiple towers leading to triangulation data, and (3) the issue can be raised later in the context of a motion to suppress.[17] In other words, the information obtained is insufficient to presently pinpoint a particular individual and his or her location.

Courts rejecting government applications have focused on the absence of explicit standards in the relevant statutes, [18] the Pen Register Statute (PRS)[19] and the Stored Communications Act (SCA).[20] These courts have also expressed concern that the government might use the information to make the cell phone a "tracking device." These courts cite congressional testimony from the former director of the Federal Bureau of Investigation about certain aspects of the PATRIOT Act that purportedly limited the use of the statutes at issue for cell-phone monitoring applications. These cases find that the applicable standard is probable cause under Rule 41 of Federal Rules of Criminal Procedure and that the government has not made this showing, thus refusing to issue the authorization.

Other cases granted the government's application.[21] Judges accepting these applications have focused on the explicit text of CALEA, which states that cell-site information may not be obtained "solely pursuant" to the Pen Register Statute.[22] These courts permit the government to obtain cell-site information after meeting the requirements of both the PRS and § 2703 of the SCA. These courts point out that Section 2703 of the SCA fulfills the purpose of Section 1002 exception, to require more than the minimal authorization imposed under the PRS, but does not require a probable-cause showing. In many of these cases, moreover, the judges ensured that the orders authorized only limited information, minimizing the concern that a cell phone could be used as a kind of "tracking device."

A brief survey of cases and issues will be discussed below.

---

[17] *See, e.g.*, In Re Application of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d), 509 F. Supp. 2d 76, 80-81 (D. Mass. 2007) (hereinafter "Massachusetts Opinion").

[18] *See*, e.g., In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Info., 407 F.Supp.2d 132 (D.D.C. 2005); In the Matter of the Application of the United States of America for an Order (1) Authorizing the Installation and Use of a Pen Register and 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) (hereinafter "Orenstein Opinion II").

[19] 18 U.S.C. §§ 3121-27

[20] 18 U.S.C. § 2703.

[21] *See*, In the Matter of the Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Info. and/or Cell-Site Info., 411 F.Supp.2d 678 (W.D.La.2006); In the Matter of the Application of the United States of American for an Order Authorizing the Installation and Use of a Pen Register and Caller Identification System on Tel. Nos. [Sealed] and [Sealed] and the Prod. of Real Time Cell Site Info., 402 F.Supp.2d 597 (D.Md.2005).

[22] 47 U.S.C. § 1002(a)(2). *See*, In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information, 497 F. Supp. 2d 301, 307 (D. Puerto Rico 2007) (hereinafter "Puerto Rico decision").

Cell-Site Information is Protected by the Fourth Amendment and the Government Must Obtain a Warrant Based Upon Probable Cause

Currently, the Third Circuit Court of Appeals is considering a district court's denial of the government's request to obtain cell-site location information concerning a subscriber that was living in another state and linked to large-scale narcotics trafficking, evading visual surveillance. The district court rejected the government's application, and affirmed the magistrate's order requiring a warrant based on probable cause.[23] In an extensive opinion, the Magistrate denied an *ex parte* application by the government pursuant to the SCA. The court addressed whether the government could obtain an order for certain cell phone information that disclosed the user's location without showing probable cause. The government contended that it could obtain such an order based on a reasonable belief that such information was relevant to a criminal investigation under the SCA. The court concluded that the SCA, whether alone or in tandem with other statutes, did not authorize access to an individual's cell-phone-derived location information, either past or prospective, on a simple reasonable relevance standard. The court held that the SCA expressly set movement/location information outside its scope by defining "electronic communications" to exclude any communication from a tracking device. It also found that other statutes cited by the government did not drop the Fourth Amendment requirements and that legislative history made clear that Congress was not seeking to amend the background standards, such as probable cause, governing disclosure of tracking information. The court thus denied the government's requests for cellular-telephone-derived location information, historic or prospective, absent a showing of Fourth Amendment probable cause.

On appeal, the government maintains that since § 2703(d) allows for the compelling of a record pertaining to a subscriber, by a provider of an electronic communication service, historical cell-site usage information falls within the statute's ambit. The government also contends that this information falls clearly within the Stored Communications Act's (SCA) plain language. Under the government's reasoning a cell phone company is a provider of electronic communication service, because it provides users the ability to send or receive wire or electronic communications, and cell-site information is a record pertaining to a subscriber without providing the content of the information of the call.[24]

The government also maintains that the district court conflated the historical and *prospective* use of cell phones. As such, they maintain that CALEA (47 U.S.C. § 1002) does not apply because the information is not being acquired *solely pursuant* to the authority for pen registers and trap and trace devices. The government relies on the separate authority in the SCA, and CALEA did not intend to incorporate the provisions of the SCA in its provisions.[25] CALEA, as well as the Wiretap Act and pen register statute,

---

[23] 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, 534 F. Supp. 2d 585 (W.D. Pa. 2008). The principal object of the Fourth Amendment is the protection of privacy and people rather than property and places. In *Katz v. United States*, 389 U.S. 347-353 (1967), the Court stated that "[T]he test propounded . . . is whether there is an expectation of privacy upon which one may "justifiably" rely." That is, the capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was reasonable expectation of freedom from governmental intrusion. This reasonable expectation must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law, or to understandings that are recognized and permitted by society. Rakas v. Illinois, 439 U.S. 128 (1978). When the Fourth Amendment protects information it protects that information with a probable cause standard and particularity backed by the exclusionary rule.

[24] *See* Brief of Government, p. 11 (citing "Gorenstein Opinion", 405 F.Supp. 2d 435, 444).

[25] The Government cites the *expressio unius est exclusio alterius* canon for its proposition. The expression of one is the exclusion (continued...)

regulates exclusively prospective, ongoing surveillance. The SCA conversely handles historical communications and thus its different mechanism for obtaining records, a subpoena, is applicable. Appellee's arguments that a magistrate can demand probable cause under the SCA, according to the government, violates the plain language of the statute.[26]

Historical cell-site information, the government argues, is also not a communication from a tracking device because it is not an electronic communication, it is information from a cell-phone which is a wire communication since it involves the human voice. According to the Government, communication cannot be both electronic and wire in nature.[27] Attempting to distinguish a cell-phone from a tracking device, the government argues that a homing device is installed by the government, and the ECPA embraces only the narrow terms of when the government applies to have a tracking device installed. The government maintains that electronic tracking devices are defined separately from cellular telephones in the ECPA and cellular telephones are protected as communications under the Wiretap Act and Stored SCA.[28] A contrary result, according to the government, mitigates the privacy protections given to cellular telephones under the Wiretap Act, such as in text messages or email.

Regarding the Fourth Amendment, the government maintains there is no reasonable expectation of privacy and cites *U.S. v. Miller*, 425 U.S. 436 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979). It maintains that the information is far too imprecise and in the possession of a third party, the telephone company. Thus it is not the individual's private information but information handled by the company internally and not typically known by the customer. Even if found to have a greater link to the customer, the government states that the information is like that of a dialed telephone number, essential information for the telephone call to be completed and voluntarily turned over. The government also distinguishes the GPS beeper cases because the monitoring is analogous to the monitoring of beeper signals that do not reveal facts about the interior of a constitutionally protected space. The user's exact location is not discerned.[29]

Appellee maintains that a warrant founded upon Fourth Amendment probable cause, or an exception to the warrant requirement, is necessary. Responding to the government, appellee maintains that, (1) the information is far more precise than the government asserts and can be used to reconstruct a user's exact location through triangulation and GPS technology; (2) the public has manifested a subjective expectation of privacy in cell-phone records through polling showing a desire for a warrant requirement and it is objectively reasonable due to the pervasive role cell-phones play in daily lives as well as the hidden, continuous, indiscriminate, and intrusive monitoring which takes places requiring extensive judicial oversight;[30] (3) the case law cited by the government does not create a third party exception because the

(...continued)

of the other, which it maintains does not reach an absurd result due to the necessity of the different evidentiary thresholds (certification of relevance for pen register v. specific and articulable facts for the SCA).

[26] *See* Government's Reply Brief at 11-15 (discussing the limiting term "only" in the statute).

[27] 18 U.S.C. §§ 2510(1), (12)(A) (2006).

[28] *See* Government's Brief, 18-20, 22 (citing 18 U.S.C. § 3117, "Massachusetts Opinion," 509 F. Supp. 2d 76; "Gorenstein Opinion," 304 F. Supp. 2d 435 (S.D.N.Y. 2005); and the legislative history of the EPCA).

[29] United States v. Knots, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

[30] Brief of Appellee at 7-9 (describing how the process of retrieving the cell-history information meets the factors elucidated and citing Berger v. New York, 388 U.S. 41 (1967) as well as United States v. Tores, 751 F.2d 875 (7th Cir. 1984)).

case law involved third parties that had greater control over the information, making their situation more akin to a second party transaction;[31] and (4) the information is not kept in the normal course of business.

Cell-Site Information is Subject to Rule 41 Because a Phone is a Tracking Device Requiring Probable Cause

There have been two highly cited opinions out of the Eastern District of New York. In the first opinion, the court held that cell-site information, even when referencing a single cell tower, does not fall within the SCA, and "is not information that the government may lawfully obtain, absent a showing of probable cause."[32] The standard under the SCA for such an order is "specific and articulable facts showing that there are reasonable grounds to believe that [such information is] relevant and material to an ongoing criminal investigation."[33] The magistrate concluded that cell-site information was not an electronic communication because tracking devices are excluded from the definition of an electronic communication under the SCA.[34] While the phone itself is not a tracking device, the authorization "would effectively allow the installation of a tracking device without the showing of probable cause normally required for a warrant."[35] While the government's application for a pen register in the context of cell-site history information falls within the pen register statute's express terms as "routing, addressing, and signaling information,"[36] the CALEA prohibits the disclosure by a telecommunications carrier of "any information that may disclose the physical location of the subscriber"[37] *solely* on the basis of a pen-register or trap and trace, on anything less than probable cause.[38] This reflects the Congress' concerns about infringing individual Americans' privacy rights.[39]

In a second opinion, the magistrate again rejected the government's application, upon request of reconsideration, again citing the CALEA and its legislative history as prohibiting access to the cell-site information based solely on the authority of a pen-register or its combination with the SCA.[40] The magistrate heavily relied on a decision from the U.S. District Court for the Southern District of Texas, in expanding upon its rejection of the government's application.[41] He found that not only was the information from a tracking device, excluding it as an electronic communication under the SCA, but also that the record does not "involve the transfer of the human voice."[42] Thus it also could not be a wire

---

[31] *See* Appellee's Brief at 16.

[32] "Orenstein Opinion I," 384 F. Supp. 2d 562, 564.

[33] "Orenstein Opinion I," 384 F. Supp. 2d at 563 (citing 18 U.S.C. § 2703(d) (2006)).

[34] *See Id.* at 564. *See also* 18 U.S.C. §§§ 2711(1), 2510(12), 3117 (2006). A tracking device is defined broadly as "an electronic mechanical device which permits the tracking of movement of a person or object." 18 U.S.C. § 3117(b) (2006).

[35] *Id.*

[36] 18 U.S.C. § 3127(3), (4) (2006).

[37] 47 U.S.C. § 1002(a)(2)(B) (2006).

[38] "Orenstein Opinion I," 384 F. Supp. 2d at 565. This would take the form a Rule 41 probable cause order. *See* "Smith Opinion I," 396 F. Supp. 2d at 751-53.

[39] *Id.* (citing the House Judiciary Committee Report on CALEA and the testimony of former FBI Director Louis Freeh stating "the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information other than that which can be determined from the phone number").

[40] "Orenstein Opinion II," 396 F. Supp. 2d 295, 306-07.

[41] "Smith Opinion I," 396 F. Supp. 2d 747.

[42] "Orenstein Opinion II," 396 F. Supp. 295, 308.

communication.[43] The court also maintained that the SCA could not pull the government out of the "solely pursuant" language of the CALEA because of the profound structural differences between the SCA and electronic surveillance statutes. The magistrate wrote, "Congress did not intend the former to be a vehicle for allowing prospective, real-time surveillance of a mobile telephone user's physical location and movement during the course of a call."[44] He also concluded that the SCA did not apply to relieve the prohibitions of CALEA because the SCA did not change "existing surveillance capabilities."[45] Regarding the pen-register statute, the magistrate maintained that the "signaling information" provisions of the pen-register statute were merely to reach electronic communications, such as email, not cell-site information.[46] As such, according to the magistrate a showing of probable cause was necessary by the government.[47]

The SCA's applicability to purely historical cell-site information, however, seemed to be left open by the magistrate to the SCA's lower threshold.[48] Yet the decision noted even if granted, this only authorizes a provider to disclose the information, not the interception of such information by law enforcement.[49]

Similar to the cases from the Eastern District of New York, a U.S. district court from the Southern District of Texas has rejected the Government's hybrid order theory. The court maintained that the PRS is not the exclusive mechanism by which the government can retrieve cell-site information based upon the "greater includes the lesser maxim." In other words, when a showing of greater authority is asserted, such as a super-warrant under the Wiretap Act allowing for the recording of conversations, the Government is also given the lesser authority to monitor tracking devices. As such, Rule 41 could allow for the Government to access the cell-site information it desires and "is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause."[50] Removing this exclusivity of the pen-trap statute, according to the magistrate, collapses the necessity of moving to CALEA and the SCA. However even if viewed as non-persuasive, the emphasis on the word "solely" in the CALEA seems to be misplaced because it is not mentioned in the legislative history and a pen register may not be the *sole* mechanism for obtaining cell-site information.[51] Moreover, the word "solely" could be interpreted to

---

[43] *See* 18 U.S.C. §§ 2510(1), 18 (2006) (stating that a wire communication "must involve a transfer of the human voice").

[44] "Orenstein Opinion II," at 309. In coming to this conclusion Judge Orenstein rejected the Government's instantaneous storage theory that cell-site information becomes historical once captured relying on the statute's present tense phrasing to suggest that the items must already be in existence. *See* 18 U.S.C. 2703(d) (2006) ("*are* relevant and material to an ongoing investigation").

[45] *Id.* at 319-20 (citing testimony former FBI Direct Louis Freeh at the Senate Judiciary Committee "All transactional information is . . . exclusively dealt with in the SCA and . . . Congress treats law enforcement's use of pen registers and dialing information differently than transactional information.")

[46] *Id.* at 318 (citing the legislative history of the USA PATRIOT Act amendments).

[47] Judge Orenstein left open the possibility of a super-warrant for prospective monitoring of cell-site information in future litigation but did not decide the issue. *See id.* at 322, 324-25.

[48] *Id.* at 312-13 ("I have no quarrel, that a court may properly, under § 2703, compel a provider to disclose historical cell site information about past calls that it currently has in electronic storage"). The U.S. District court in Massachusetts when analyzing an application for purely historical cell-site information did in fact approve its use under the SCA because the record holder cell-phone company is a provider of an electronic communication service, the cell-site data is a record pertaining to a subscriber in that it is stored or archived by the cellular company, and the information is not content information disclosing any substance of the call itself. *See* "Massachusetts Opinion." *See* "Puerto Rico Decision" for *contra* result when assessing cell-site information in the context of the SCA and whether it constitutes a "record."

[49] *Id.* at 314-15.

[50] In the matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 830 (S.D.T.X. 2006) (hereinafter "Smith Opinion II") (citing United States v. New York Tel. Co., 434 U.S. 159 (1977)).

[51] *Id.* at 832-33 (discussing an analogy that a law degree may not be sufficient to practice law as an additional passage of the bar (continued...)

embrace the hierarchy of electronic surveillance law, in that greater showings are necessary due to the information requested. While "some amount of legal process will be necessary to obtain location information, certification of relevance . . . is not enough."[52] Without the word "solely" according to the court, CALEA could be erroneously interpreted that no amount of process would access the cell-site information.[53] Finally, in regards to the SCA, the court cites the SCA's clear statutory prohibition of a phone company "disclosing subscriber information to any governmental entity except under certain carefully delineated circumstances."[54] Six exceptions are listed and none include or implicate the pen-register statute.

Cell-Site Information Requires a Pen Register and § 2703 of the Stored Communications Act Despite the Prohibitions of CALEA

A minority of courts have held that the government need not establish probable cause under Rule 41 to access cell-site information. The most cited of these opinions is from the Southern District of New York.[55] In allowing for the cell-site information based upon the "reasonable and articulable facts," provision of the SCA, the court highlighted that the information would not be gleaned while the telephone was not on a phone call and was only from one cell tower, mitigating the possibility of triangulation data. In reference to the CALEA terms that prohibits monitoring "solely pursuant" to a pen register, the court maintained that this meant that a pen register could be combined with some other form of statutory authority, which the SCA satisfied because it is more than the minimal authorization of a pen-register order. The court was careful to limit its holding to information coming from a single tower, from the user's particular telephone, and transmitted by the provider to the government.[56]

Conclusion

A majority of jurisdictions have found the probable cause standard of Rule 41 applicable for government access to cell-site information. These courts appear to differentiate between historical information and prospective monitoring. However, other jurisdictions have held that a mere showing of reasonable and articulable facts is sufficient. Further litigation, particularly in the Court of Appeals, may clarify the issue.

(...continued)

is required, but also that a law degree may not be *necessary* to practice law as some states allow individuals to sit for the bar after informal study).

[52] *Id.* at 833.

[53] *Id.*

[54] *Id.* at 834 (citing 18 U.S.C. § 2703(a)(3) (2006).

[55] "Gorenstein Opinion," 405 F. Supp. 2d 435.

[56] This ruling was expanded to encompass prospective cell-history information and the tracking device exception to the SCA was rejected because cell phones are not installed but carried and used voluntarily. *See* In the Matter of Application of U.S. for an Order for Disclosure of Telecommunications Record and Authorizing the Use of a Pen Register and Trap and Trace, 411 F. Supp. 2d 678 (W.D. La. 2006).