ValpoScholar Valparaiso University Law Review

Volume 41
Number 4 *Symposium on Electronic Privacy in the Information Age*

*pp.*1413-1480

Symposium on Electronic Privacy in the Information Age

Cell Phones as Tracking Devices

M. Wesley Clark

CELL PHONES AS TRACKING DEVICES

M. Wesley Clark*

I. INTRODUCTION

With the advent of the ubiquitous cell phone, law enforcement has been handed a priceless investigative tool without the outlay of any Federal funds for the hardware. Prior to the rapid rise in cell phone use, the Drug Enforcement Administration ("DEA"), for example, would use traditional tracking equipment[1] that it owned (or borrowed) and would have to surreptitiously install it, typically on or in a vehicle, aircraft, or boat or secreted in containers carrying precursor chemicals needed to manufacture controlled substances.

The great advantages of cell phone tracking are (1) that many if not most adults have at least one cell phone (thus permitting the tracking of countless individuals as opposed to following only the travels of a much more limited class of conveyances[2] and drums of chemicals); and (2) law enforcement is spared the legal and tactical hurdles that are often encountered when seeking to *install* the tracking devices.

---

* Mr. Clark is a Senior Attorney with the Office of Chief Counsel, Drug Enforcement Administration, and an adjunct professor at George Mason University, teaching "Surveillance and Privacy in Contemporary Society." The views expressed herein are his and do not reflect the views of the DEA Office of Chief Counsel, DEA, or the Department of Justice. This Article is an expansion of one appearing in the May 2006 FBI LAW ENFORCEMENT BULLETIN, titled *Cell Phone Technology and Physical Surveillance*.

1 Even government-owned tracking devices are undergoing modernization in the 21st century, moving from radio tracking devices to those utilizing the more precise satellite global positioning system ("GPS"). GPS tracking by law enforcement has been upheld on the same basis as the older, more traditional, radio-based tracking equipment. *See* United States v. Moran, 349 F. Supp. 2d 425, 467-68 (N.D.N.Y. 2005). For a further discussion of GPS tracking, see *infra* note 330 and accompanying text. Note, however, that today "the traditional homing devices . . . are now monitored via radio signals using the same cell phone towers used to transmit cell site data." *In re* the Application of the U.S.A. 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, 402 F. Supp. 2d 597, 604 (D. Md. 2005) [hereafter DMD#1].

2 If the suspect leaves or changes the conveyance to which a tracking device has been affixed, law enforcement has lost the ability to electronically determine the surveillance target's location. Assuming the suspect has not passed off the cell phone to someone else, this is not the case with cell phone tracking. Cell phone service providers whose instruments do not contain GPS chips were directed by the FCC to "be able to pinpoint 67 percent of calls within 100 meters and 95 percent of calls within 300 meters." *DMD#1,* 402 F. Supp. 2d at 599 (citing 47 C.F.R. § 2018(h)(1)(2005)).

Case law was supposedly well-settled after two Supreme Court cases decided in the 1980s, *United States v. Knotts*[3] and *United States v. Karo*.[4] These cases held that so long as the conveyance or "thing" to be *monitored* is out and about on "public thoroughfares,"[5] "open fields," or even on private property[6]—all instances where the information revealed by the surveillance target could be observed by visual surveillance engaged in by third parties—no showing of any evidence, let alone probable cause, is required.[7] This, of course, does not present a problem, so long as the tracking equipment belongs to the government, but it does present a very real issue when third-party assistance is necessary to conduct the monitoring.

The rub is that cell phone companies, concerned about potential liability, will not furnish cell phone location information to law enforcement absent a court order. The legal issue of the moment relates to the proper quantum of evidence that the government must demonstrate to a court before such an order for *prospective* (or real-time)[8] data will be given.

---

3 460 U.S. 276 (1983).

4 468 U.S. 705 (1984).

5 "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another . . . . [The subject] voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property." *Knotts*, 460 U.S. at 281-82.

6 "[N]otions of physical trespass based on the law of real property [are] not dispositive . . . ." *Id.* at 285.

7 Probable cause to monitor will be required if electronic tracking is to occur within a private dwelling, i.e., a "location not open to visual surveillance," or—assuming it too is not open to visual surveillance—its curtilage. *Karo,* 468 U.S. at 714-15. (A thorough discussion of "curtilage" is outside the scope of this Article.)

8 It is submitted that for other than stored, previously-acquired cell site location data, "real-time" and "prospective cell site information" are conceptually the same thing: permission is being sought to obtain "yet-to-be" information that is to be acquired/become available during a span of time that is to occur after an authorizing court order would be signed. However, one court has suggested that the two terms can mean different things:

> 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. Records stored by the wireless 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.

DMD#1, 402 F. Supp. 2d 597, 599 (D. Md. 2005).

In a 2004 cell phone tracking case, *United States v. Forest*,[9] DEA already had authority to intercept wire communications pursuant to Title III[10] (18 U.S.C. §§ 2510-2522). Additionally, the Title III order directed the provider "to disclose to the government all subscriber information, toll records, and other information relevant to the government's investigation."[11] As an aid to the establishment of visual contact with the subject, DEA dialed the target's cell phone (without letting it ring) several times in the course of the day and would then obtain the cell phone location information from the service provider.[12]

Among other things, the defendant argued that in so doing, DEA violated his Fourth Amendment rights. Of course the threshold question was whether or not securing the cell site location information constituted either a search or a seizure. For that to be the case, there must have first been a "subjective expectation of privacy that society recognizes as reasonable"; but that was not the situation in *Forest* because the data "was used to track [the target's] movements only on public highways."[13] The Sixth Circuit thus concluded that *Knotts* was controlling and that there was "no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following [the target's] car."[14]

But in most location surveillance scenarios, law enforcement will probably not be fortunate enough to have a Title III order up and running, like in *Forest*, thus presenting the need for a stand-alone order. To obtain such court authorization, the Department of Justice ("DOJ") has been using selected provisions from Title II of the Electronic Communications Privacy Act ("ECPA"),[15] primarily 18 U.S.C. § 2703(d),

---

9 355 F.3d 942 (6th Cir. 2004), *cert denied,* 543 U.S. 856 (2004).

10 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968) (codified at 18 U.S.C. §§ 2510-2522 (2000)).

11 *Forest,* 355 F.3d at 947.

12 DEA used the carrier's "computer data to determine which cellular transmission towers were being 'hit' by [the target's] phone. This 'cell-site data' revealed the general location of [the target]." *Id.*

13 *Id.* at 950-51.

14 *Id.* at 951. "Although the DEA agents were not able to maintain visual contact with [the target's] car at all times, visual observation was *possible* by any member of the public. The DEA simply used the cell-site data to 'augment[ ] the sensory faculties bestowed upon them at birth,' which is permissible under *Knotts* . . . . [T]he cell site data is simply a proxy for [the target's] visually observable location." *Id*.

15 Pub. L. No. 99-508, 100 Stat. 1848, 1860 (2000). Note that 18 U.S.C. §§ 2701-2712 (Title II of the ECPA, as amended) is sometimes informally referred to as the Stored Communications Act or SCA, even though it is not denominated as such within the body of the ECPA.

either alone or in combination with the pen register/trap and trace statute ("Pen/Trap Statute"), 18 U.S.C. §§ 3121-3127.[16]

This has not proved to be a winning strategy, however, and DOJ is (depending upon how one keeps score and as of this writing) 0-17-5 or 5-17 in a series of late 2005-early 2007 federal cases before twelve United States Magistrate Judges ("USMJs") and five District Court Judges in twelve different judicial districts (California; two in Indiana; Louisiana; Maryland; three in New York; Texas; Washington, D.C.; Wisconsin; and West Virginia).[17] In the course of their decisions, most of the courts

---

[16] Prior to passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 212 (2001), "pen register" was defined as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached[.]" Before the advent of cell phones (at a time when telephones were connected by copper wires), a pen register was actually a machine that printed onto a roll of paper all number dialed from the targeted phone. It would also print the times that the telephone receiver was picked up ("off hook") and when it was replaced ("on hook"). *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979). Today most of the data that the machines used to acquire and print out are collected and arranged by service provider computer feeds and software. "[I]nformation that was heretofore captured by a pen register can now be transmitted digitally by the telephone service provider." *In re* the Application of U.S.A. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace Device, 405 F. Supp. 2d 435, 438 n.1 (S.D.N.Y. 2005) [hereinafter SDNY#1]. In recognition of this technology shift, § 216 of the USA PATRIOT Act updated the pen register definition (and, relatedly, that of the trap and trace "device" as well) so that § 3127(3) now describes a pen register as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted[.]" 18 U.S.C. § 3127(3) (2000 & Supp. IV 2005).

[17] In addition to *DMD#1,* 402 F. Supp. 2d 597 (D. Md. 2005), and *SDNY#1,* 405 F. Supp. 2d 435 (S.D.N.Y. 2005), these are: *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 Information and/or Cell Site Information, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) [hereinafter EDNY #1], *on reconsideration*, 396 F. Supp. 2d 294 [hereinafter EDNY #2]; *In re* the Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005) [hereinafter SDTX#1]; *In re* the Applications of U.S.A. for Orders Authorizing the Disclosure of Cell Cite Information, Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) [hereinafter DDC#1]; *In re* the Application of U.S.A. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D.D.C. 2005) [hereinafter DDC#2]; *In re* the Application of U.S.A. for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134 (D.D.C. 2006) [hereinafter DDC#3]; *In re* the Application of U.S.A. for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947 (E.D. Wis. 2006) [hereinafter EDWIS#1]; *In re* the Application of U.S.A. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 411 F. Supp. 2d 678 (W.D. La. 2006) [hereinafter WDLA]; *In re*

concluded that an order based upon probable cause and grounded upon Federal Rule of Criminal Procedure 41 ("Rule 41") is required to compel cell phone providers to divulge real-time/prospective cell site location information.[18]

---

the Application of U.S.A. for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification Number (585) 111-1111 and the Disclosure of Subscriber and Activity Information Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) [hereinafter WDNY]; *In re* the Application of U.S.A. for an Order Authorizing the Installation and Use of a Pen Register with Caller Identification Device and Cell Site Location Authority on a Certain Cellular Telephone, 415 F. Supp. 2d 663 (S.D. W. Va. 2006) [hereinafter SDWVA]; *In re* the Application of U.S.A. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed], 416 F. Supp. 2d 390 (D. Md. 2006) [hereinafter DMD#2]; *In re* the Application of U.S.A. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, No. 06 CRIM. MISC. 01, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) [hereinafter SDNY#2]; *In re* the Application for an Order Authorizing the Installation and Use of a Pen Register Device, Trap and Trace Device, Dialed Number Interceptor, Number Search Device, and Caller Identification Service, and the Disclosure of Billing, Subscriber, and Air Time Information, No.S-06-SW-0041 (E.D. Cal. Mar. 15, 2006) [hereinafter EDCA]; *In re* the Application of U.S.A. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, 433 F. Supp. 2d 804 (S.D. Tex. 2006) [hereinafter SDTX#2]; United States v. Bermudez, No. IP 05-43-CR-B/F, 2006 WL 3197181 (S.D. Ind. June 30, 2006) [hereinafter SDIND]; *In re* the Application of U.S.A. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services; *In re* the Application of U.S.A. for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Location of Cell Site Origination and/or Termination, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006) [hereinafter NDIND]; *In re* the Application of U.S.A. 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 (S.D. Tex. 2006) [hereinafter SDTX#3]; *In re* the Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the Number [SEALED], 439 F. Supp. 2d 456 (D. Md. 2006) [hereinafter DMD#3]; *In re* the Application of U.S.A. for an Order Authorizing the Disclosure of Prospective Cell Site Information, No. 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) [hereinafter EDWIS#2]; *In re* the Application of U.S.A. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) [hereinafter SDNY#3]; *In re* Application for an Order Authorizing the Extension and Use of a Pen Register Device, No. 07-SW-034 GGH, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007) [hereinafter EDCA#2].

[18] This is not to conclude that legal underpinnings other than 18 U.S.C. §§ 2703 and §§ 3121-3127 or FED. R. CRIM. P. 41 are not available upon which to ground an application for an order compelling a cell phone service provider to provide real-time/prospective cell site location information. *See* discussion *infra* note 99; *infra* Part III.A (*Alternative Legal Foundation*).

II. BACKGROUND AND CASES

A. Eastern District of New York—August and October, 2005 (EDNY#1/EDNY#2)

Underpinning its application with 18 U.S.C. §§ 2703(c)(1)(B), (c)(2), and (d), the U.S. Attorney's Office ("USAO") sought an order compelling the "disclosure of the location of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and if reasonably available, during the progress of a call, for the Subject Telephone."[19] Of these three subsections,[20] the USMJ found that only one, § 2703(d), might provide a basis for the order sought. An order pursuant to that provision can be had upon a showing of "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."[21]

The USMJ concluded that the government had provided the requisite level of evidence called for by § 2703(d) and that under the statutory definition,[22] cell site location information would, in fact, constitute the "contents of . . . [an] electronic communication" except for one thing: the definition of "electronic communication"[23] specifically excludes "any communication from a tracking device,"[24] the latter term being defined at 18 U.S.C. § 3117(b) as "an electronic or mechanical device which permits the tracking of the movement of a person or

---

19 *EDNY#1*, 384 F. Supp. 2d at 563.

20 18 U.S.C. § 2703(c)(1)(B) provides that the government may require "[a] provider of electronic communication service or remote computing service [to] disclose a record or other information pertaining to a subscriber to or customer of such service . . . [when the Government obtains a court order pursuant to § 2703(d)]." An "electronic communication service," the term relevant for our purposes, is "any service which provides to users thereof the ability to send or receive wire or electronic communications[.]" *Id.* § 2510(15). Cell phone calls are a type of "wire communication." Section 2703(c)(2) provides that electronic communications services and remote computing services "shall disclose to a governmental entity the—(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)" if the government obtains, *inter alia,* an order pursuant to § 2703(d).

21 *Id.* § 2703(d).

22 *See id.* § 2510(12) (defining electronic communication by operation of 18 U.S.C. § 2711(1)).

23 *Id.*

24 *Id.* § 2510(12)(C).

object." The USMJ determined that based upon the statutory definitions, the targeted cell phone equated to—and was thus "precisely describe[d]" as—a tracking device. Thus the court felt it was constrained from granting the government's application for a tracking order to the extent the pleading was based upon 18 U.S.C. § 2703.

Because the government's application also sought permission to conduct pen register as well as trap and trace operations, the court felt that "[i]n fairness . . . [it] must also consider whether the relief is available simply by virtue of the government's otherwise proper application . . . " for this additional authority.[25] The USMJ concluded the Pen/Trap statute did not provide such a basis because specific language in the Communications Assistance for Law Enforcement Act ("CALEA")[26] precluded it. Among other things, CALEA mandated that telecommunications carriers be technologically able to

> expeditiously isolat[e] and enabl[e] the government, pursuant to a court order or other lawful authorization, to access call-identifying information . . . except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . , such call-identifying information shall not include any information that may disclose the physical location of the subscriber . . . .[27]

Distilling matters, the USMJ opined that "where a carrier's assistance to law enforcement is ordered on the basis of something less than probable cause, such assistance must not include disclosure of a subscriber's physical location."[28] Upon reconsideration, the USMJ again

---

[25] EDNY#1, 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005). It should be kept in mind that the government never grounded its request for cell site location information upon 18 U.S.C. §§ 3121-3127. Note that after *EDNY#1*, but before *EDNY#2*, *SDTX#1* was issued. The USMJ who decided *EDNY #1* and *EDNY#2* ". . . considered precisely the same statutes and legislative history as [did the *SDTX#1* USMJ] (and apparently many of the same arguments), and . . . independently arrived at the same conclusions as did he." EDNY#2, 396 F. Supp. 2d 294, 304 (E.D.N.Y. 2005).

[26] Pub. L. No. 103-414, § 103, 108 Stat. 4279, 4280-81 (1994) (codified at 47 U.S.C. § 1002(a)(2)(B) (2000)).

[27] 47 U.S.C. §§ 1002(a)(2)(B).

[28] *EDNY#1*, 384 F. Supp. 2d at 565. To the extent the government seeks a cell phone user's location based upon the Pen/Trap Statute, this is correct. However, and despite the USMJ's discussion in *EDNY#2*, 396 F. Supp. 2d at 325-26, a strong argument exists that such information can be obtained from carriers based upon a less than probable cause order issued pursuant to FED. R. CRIM. P. 57 and the All Writs Act, 28 U.S.C. § 1651 (2000). 18 U.S.C. § 3117(a) states in pertinent part that ". . . a court is empowered to issue a warrant

denied the government's request for real-time cell site location information again concluding that the existing law did not allow the government to obtain the information "on a prospective, real-time basis without a showing of probable cause."[29]

B. Southern District of Texas – October 2005 (SDTX#1)

In the Texas case, the government specifically combined a pen/trap request with one seeking subscriber records—as the latter term is described at 18 U.S.C. § 2703(c)(2). The application also sought, in part, the prospective/real-time "location[30] of cell site/sector (physical address) at call origination (for outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call."[31] In addition to this, however, the request also asked for more than had been requested in the *EDNY #1* application: "information regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture."[32] As a result, the question that the USMJ found himself faced with was whether "this location information [is] merely another form of subscriber record accessible upon a showing of 'specific and articulable facts' under 18 U.S.C. § 2703(d), as the government contends[,] . . . [or whether] this type of surveillance require[s] a more exacting standard, such as probable cause under Federal Rule of Criminal Procedure 41[.]"[33]

---

or other order for the *installation* of a mobile tracking device[.]" (emphasis added). Note that although the government invoked both the Pen/Trap Statute and 18 U.S.C. § 2703(d), it "identifies no other method for its agents to obtain the information it seeks[.]" *EDNY#1,* 384 F. Supp. 2d at 566.

29 *EDNY#2,* 396 F. Supp. 2d at 295. Note that upon his reconsideration, which included a second, perhaps closer look at the government's proposed applications and orders, the USMJ changed his earlier conclusion—which was that the government was asking the cell phone carrier to surrender cell site location information—to one that construed the government's request to be one seeking authority to use a pen register to acquire the data "and not through any actual disclosure from a provider of electronic communications service[,]" but this was not significant because "Congress plainly intended the 'location' prohibition in CALEA to regulate not only what a carrier can provide, but also what law enforcement can lawfully 'obtain.'" *Id.* at 307 n.9.

30 At an earlier time, the court appears to have granted a government application for historical cell site data. SDTX#1, 396 F. Supp. 2d 747, 748 (S.D. Tex. 2005). For a description of the interaction between cell phones and cell phone towers, see *id.* at 750.

31 *Id.* at 749. This is exactly the same language used in the *EDNY#1* application.

32 *Id.*

33 *Id.* at 749-50.

At the end of the day, the court in *SDTX#1* came to the same conclusion as the USMJ in *EDNY#1* and *EDNY#2* and rejected all of the government's theories—Pen/Trap, Stored Communications Act ("SCA"),[34] and the hybrid mix of the two.[35] The USMJ ended his opinion by observing that "[d]enial of the government's request for prospective cell site data in this instance should have no dire consequences for law enforcement. This type of surveillance is unquestionably available upon a traditional probable cause showing under Rule 41."[36]

C. District of Maryland – November 2005 (DMD#1)

In the Maryland case, the government again raised its combined Pen/Trap-SCA hybrid theory and suffered the same result: "[The first two USMJs] reject[ed] this 'hybrid theory' under almost identical rationales. . . . This court joins them."[37] Although the outcome for the government was the same as in the earlier USMJ opinions, the court here at least helpfully recognized, but to no effect, that if obtaining real time cell site information is the same as obtaining a tracking device, then the government is likely not "constitutionally required to obtain a warrant" so long as the phone is in a public place and visual surveillance is possible.[38] This was because in the final analysis,

> 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

---

34 *See infra* note 90 and accompanying text.

35 The government's "hybrid" theory is explained well by the court in *SDTX#1,* 396 F. Supp. 2d at 761. Summarizing, this construct approach proceeds from the realization that CALEA precluded use "solely" of the Pen/Trap Statute to obtain prospective/real-time cell site location information, 47 U.S.C. § 1002(a)(2), thus necessitating the conjunctive use of at least one more statute, i.e., 18 U.S.C. § 2703(c), which permits acquisition of non-content subscriber information, such as—arguably—cell site location information.

> By mixing and matching statutory provisions in this manner, the government concludes that cell site data enjoys a unique status under electronic surveillance law—a new form of electronic surveillance combining the advantages of the pen/trap law and the SCA (real-time location tracking based on less than probable cause) without their respective limitations.

SDTX#1, 396 F. Supp. 2d at 761.

36 *SDTX#1,* 396 F. Supp. 2d at 765.

37 DMD#1, 402 F. Supp. 2d 597, 600 (D. Md. 2005).

38 *Id.* at 604.

> may not monitor an electronic tracking device in a private place without a warrant.[39]

D. District of the District of Columbia – October and December 2005; January 2006 (DDC#1/DDC#2/DDC#3)

Facing the *SDTX#1* and both *EDNY* decisions, the government unsuccessfully tried in *DDC#1* to marry the SCA with the Pen/Trap statute. However, this approach suffered the same fate as it had in the earlier Texas and New York decisions. The mixture of the SCA and the Pen/Trap statute, wrote the USMJ, "has been rejected by two courts for reasons which . . . [this court] finds compelling. . . . [This court has] determined that the disclosure of cell cite [*sic*] information is not authorized by Section 2703, by Sections 3122 and 3123, or by any combination of the two provisions."[40] The deciding USMJ went on to state that two other USMJs in the district, including USMJ Facciola, the author of *DDC#2* and *DDC#3*, shared the same views.[41] Also recognizing the *SDTX#1* and *EDNY* opinions, but not necessarily conceding their "validity," the government in *DDC#2* attempted an unholy union of the Fourth Amendment and 18 U.S.C. § 2703(d)[42] and sought to "demonstrat[e] probable cause to believe that the requested prospective cell cite [sic] information is relevant and material to an ongoing criminal investigation."[43] More specifically, the USMJ in *DDC#2* found that this formulation was "tautological," and, in the court's analogy, that the attempt was akin to designing a horse by a committee and instead constructing a camel.[44] The court determined that "the probable cause showing does not meet the central problem identified in the [*SDTX#1* and *EDNY*] cases, that the statutes upon which the government purports to rely in those cases and in this one, *i.e.*, 18

---

[39] *Id.* at 605. This, of course, is no different from the risk the government regularly and as a matter of practice assumes when using traditional or GPS tracking devices.

[40] DDC#1, Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005).

[41] *Id.* Curiously, neither the *DDC#2* nor the *DDC#3* opinion, each written by USMJ Facciola, referred to *DDC#1*.

[42] The court appears to incorrectly see this as a somewhat bizarre blending of the Fourth Amendment with the standard articulated in 18 U.S.C. § 3122(b)(2), the Pen/Trap Statute. However, whereas 18 U.S.C. § 2703(d), part of the SCA, mandates that applicants "offer[ ] 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[,]" § 3122(b)(2) requires only that an applicant certify to the court that pen/trap information "is relevant and material to an ongoing criminal investigation[.]" DDC#2, 407 F. Supp. 2d 132, 132-33 (D.D.C. 2005).

[43] *DDC#2,* 407 F. Supp. 2d at 132-33.

[44] *Id.* at 133.

U.S.C. §§ 3122, 3123, 2703(c)(1) do not authorize the government to secure cell site data that would disclose the location of the person using the cell phone."[45]

A month later (*DDC#3*), the government returned to the same USMJ as in *DDC#2* without replacing the hybrid approach, still championing the Pen/Trap Statute in combination with the SCA. To buttress its application, the government also submitted a supporting, self-styled affidavit prepared by the investigating agent but, in the court's words, this did nothing but "put[ ] us back to where we started."[46] Referring to and following the ultimate conclusions already reached by the USMJs in Texas, New York, and Maryland, the court opined that "the standard that pertains to the issuance [of an order seeking prospective cell site location information] is, as the Fourth Amendment requires, probable cause to believe that the information sought is itself evidence of a crime, not that the information is relevant to an investigation."[47] Further, the government's proffer of "'probable cause to show relevance to an ongoing investigation'" is "an ersatz standard[.]"[48]

One of the most important matters CALEA addressed was law enforcement's continued access to the fast changing telecommunications infrastructure for the purpose of conducting lawful electronic surveillance. With the emergence of wireless technology, law enforcement did not want to be in a worse situation when attempting to engage in such surveillance than it was when telephony was accomplished only through copper wires.[49] Providers were thus required by CALEA to ensure that their deploying technologies would permit the same electronic surveillance access as before while at the same time ensuring continuing safeguards against unwarranted privacy intrusions by law enforcement under 47 U.S.C. § 1002.

Passage of the legislation, which guaranteed continued access by law enforcement—given the advent of wireless technologies—to call-identifying information via pen registers, was ensured by inserting the

---

45 *Id.*

46 DDC#3, 407 F. Supp. 2d 134, 135 (D.D.C. 2006).

47 *Id.*

48 *Id.*

49 "The purpose of . . . [CALEA] is to preserve the government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes . . . while protecting the privacy of communications and without impeding the introduction of new technologies, features, and services." H.R. REP. NO. 103-827, at 9 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489.

restriction that in no event could such data "include any information that may disclose the physical location of the subscriber[.]"[50] During consideration of the bill which became CALEA,[51] the Congressional testimony of (then) FBI Director Louis Freeh, which endorsed this restriction, was influential in securing passage.[52] The USMJ found Director Freeh's statement compelling:

> The Director's offer and its acceptance by Congress led to the exception codified as 47 U.S.C. § 1002(a)(2) . . . [T]he exception was based on the express representation by the government to Congress that the authority for pen registers and trap and trace devices would not and could not be used to secure location information, the very information the government now wants to secure by using a pen register and trap and trace device.[53]

Not only was the USMJ unconvinced that the Pen/Trap Statute provided a legal basis for acquiring cell site location information, he was similarly unpersuaded that "Congress intended to permit the government to use the Pen Register Statute to avail itself of that technology [to ascertain the location of a person using a cell phone], provided it combined its use . . . with some other means[,]" e.g., the SCA. Such a conclusion, continued the USMJ, was

> utterly counter-intuitive . . . . It is inconceivable to [the USMJ] that the Congress that precluded the use of the Pen Register statute to secure in 1994 'transactional data' . . . nevertheless intended to permit the

---

50 *Id*.

51 H.R. 4922, 103d Cong. (1994). "The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past." H.R. REP. NO. 103-827, at 22, *as reprinted in* 1994 U.S.C.C.A.N. at 3502.

52 The testimony continued,

> Therefore, H.R. 4922 includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill: . . . expressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information . . . . Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information.

H.R. REP. NO. 103-827, at 17, *reprinted in* 1994 U.S.C.C.A.N. at 3497.

53 DDC#3, 407 F. Supp. 2d 134, 138 (D.D.C. 2006).

> government to use that same statute, whether by itself or combined with some other means, to secure the infinitely more intrusive information about the location of a cell phone every minute of every day that the cell phone was on.[54]

E. Southern District of New York – December 2005 (SDNY#1)

Although the first Southern District of New York decision could be viewed as a government victory, that success is somewhat illusory because the location information sought here was relatively imprecise (hence less intrusive or invasive) when compared to the more focused data at issue in the cases already discussed. This distinction is key and was both recognized and explored not only by the USMJ in *SDNY#1* but also later by the USMJ in *DDC#3*. The *SDNY#1* USMJ granted the government's application seeking "information pertaining to the location of cell site towers receiving a signal from a particular cellular telephone," i.e., "cell site activations,"[55] and requesting that the cell phone company provide a map detailing the locations of its cell towers, i.e., their "'locations/addresses, sectors and orientations[,]'" to include "'the physical address/location of all cellular towers in the specified market.'"[56] As might be expected given the differing call volumes, there are more towers in a particular urban area than would be present in a rural area of the same size. This means that the towers will be closer to each other in the city than in outlying areas. As a rule, therefore, an operating cell phone's location can be determined with more precision when the towers in communication with the mobile phone are closer together.

---

[54] *Id.* at 140. The USMJ explains that ascertaining the location of one's cell phone (and thus the user) is more "intrusive" than obtaining the information a pen register was originally intended to secure—the numbers dialed from one's phone. *Id.*

[55] SDNY#1, 405 F. Supp. 2d 435, 436 (S.D.N.Y. 2005). "Cell site activations" refers to "'cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from a particular cellphone,'" i.e., but not during the course of the call. *Id.* at 437 (citations omitted).

[56] *Id.*

> With respect to the beginning or end of the call (and possibly sometimes in between), there is a listing [provided by the carrier] of a three-digit number assigned to a cellphone tower or base station. At least one cellular provider will give, in addition to the number of the tower, a digit ('1,' '2' or '3') indicating a 120 degree 'face' of the tower towards which the cell phone is signaling.

Id.

The *SDNY#1* USMJ took great pains to distinguish the less exact types of information being sought in the case before him from those at issue before the USMJs in the *SDTX#1, EDNY,* and *DMD#1* cases:

> First, the cell site information provided in this District is tied only to telephone calls actually made or received by the telephone user. Thus, no data is provided as to the location of the cell phone when no call is in progress. Second, at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be 'triangulated' to permit the precise location of the cell phone user. Third, the data is not obtained by the Government directly [from the user's phone] but is instead transmitted from the provider digitally to a computer maintained by the Government.[57]

The government again relied upon the Pen/Trap Statute and 18 U.S.C. § 2703. Echoing observations announced in the earlier cell phone tracking decisions, the court said that "the Pen Register Statute would by itself provide authority for the order being sought by the Government were it not for [47 U.S.C. § 1002]."[58] Not conceding that all was thereby necessarily lost, the court seized upon that portion of 47 U.S.C. § 1002(a)(2) which provides that subscriber physical location information may not be acquired "'*solely*' pursuant" to the Pen/Trap Statute. Referring to a dictionary for guidance, the USMJ reasoned that "[i]f we are told that an act is not done 'solely' pursuant to some authority, it can only mean that the act is done pursuant to that authority '*with* . . . another' authority . . . albeit in some unspecified way . . . to authorize disclosure of cell site information."[59]

The upshot of all of this is that there is "'simply impose[d] upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices.'"[60] Although attempting to determine what, exactly, constitutes an

---

57 *Id.* at 438 (explanation provided). The government computer uses software to render meaningful the raw data pushed to it by the service provider. *Id.* This distinction drawn by the USMJ with regard to the degree of precision or quality of sought-after cell phone location information strikes one as being akin to the old saw about "being a little bit pregnant."

58 *Id.* at 440.

59 *Id.* at 442 (internal citations omitted).

60 *Id.* at 443 (internal citations omitted).

appropriate "unspecified way" is "certainly an unattractive choice,"[61] the court admitted, it nevertheless began an examination of 18 U.S.C. § 2703(c)—as urged by the government—in an effort to see whether that provision would qualify. Recall that 18 U.S.C. § 2703(d) states an order pursuant to § 2703(c) may be had upon a government demonstration of "*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." [62] We know from § 2703(c) that a "record or other information" is that which "pertain[s] to a subscriber to or customer of" the communication service. Analyzing the nature of cell phone location information, the USMJ concluded that "cell site or tracking information comes within section 2703(c) and consequently is the sort of 'information' that the Government may seek pursuant to an order under section 2703(d)."[63]

In a friend of the court brief filed in the case, the Federal Defenders of New York, Inc., argued that such a § 2703(d) order could not properly issue because the statutory definition of "electronic communication" specifically excludes "any communication from a tracking device."[64] This is the same argument which the *EDNY* USMJ found sufficiently compelling to be determinative.[65] But the *SDNY#1* USMJ deflected that contention first by recognizing that a cell phone user is a consumer of "electronic communication service"; and, second, by acknowledging that such service includes a number of capabilities, i.e., a package that is *more* than just cell site information (hence, "electronic communication service" cannot be the equivalent of cell phone location information). "Inasmuch as a service that provides cellular telephone capabilities is within section

---

61 *Id.*

62 18 U.S.C. § 2703(d) (2000) (emphasis added).

63 *SDNY#1*, 405 F. Supp. 2d at 445.

64 18 U.S.C. § 2510(12) defines "electronic communication" as

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include . . . any communication from a tracking device (as defined in section 3117 of this title).

Observe that 18 U.S.C. § 2711(1) incorporates the definitions set forth at 18 U.S.C. § 2510 for purposes of §§ 2701-2712.

65 *See supra* Part II.A (discussing *EDNY#1* and *EDNY#2*).

2510(15),[66] information pertaining to a subscriber of that 'service' is obtainable under section 2703(c)."[67]

> In other words, information on the location of cell towers is not the 'service' to which a cellular customer subscribes. Instead, the user subscribes to the voice—and perhaps data-transmission capabilities provided by the cellular carrier. Although tower location information may be a necessary ingredient for the operation of that service, the 'service' to which the user subscribes is still the 'electronic communication' capabilities of the cellular telephone . . . . The exception in section 2510(12)(C) ["communication from a tracking device"] does not purport to limit the meaning of the term 'information.'[68]

The next stumbling block to confront the USMJ was whether § 2703 could be used as a basis for acquiring information created in the future. The New York Federal Defenders and the earlier USMJs "question[ed] . . . whether cell site information not yet in existence at the time of the order—that is, prospective or what is colloquially referred to as 'real time' data—may be included . . . ."[69] Indeed, chapter 121 of U.S. Code Title 18, of which § 2703 is a part, is captioned "*Stored* Wire and Electronic Communications and Transactional Records Access,"[70] thus suggesting that its provisions relate to already acquired or historical data. The USMJ put aside this concern for the moment, remarking in part that—at least in his district—cell site location information "is transmitted to the government only after it has come into the possession of the cellular telephone provider in the form of a record."[71]

---

66 18 U.S.C. § 2510(15) defines "electronic communication service" to be "any service which provides to users thereof the ability to send or receive wire or electronic communications."

67 *SDNY#1,* 405 F. Supp. 2d at 446.

68 *Id.* (citations omitted). Appreciating the mental gymnastics involved in its argument, the court conceded that "[i]t may seem anomalous that the Government may obtain under section 2703 a particular category of information pertaining to a user of electronic communications that is excepted from the term electronic communications itself." *Id.*

69 *Id.*

70 18 U.S.C. §§ 2701-2712 (2000) (emphasis added).

71 *SDNY#1,* 405 F. Supp. 2d at 447. This remark at least suggests the possibility that in districts elsewhere, cell phone location information can be provided simultaneously to both the provider and law enforcement. For a relatively recent state opinion permitting the acquisition of *historical* cell site location information, see *People v. Hall*, 823 N.Y.S.2d 334 (Sup. Ct. 2006). The court determined that a cell phone could be considered to be a

However, some of the other USMJs and the New York Federal Defenders argued that even this being so, the government was not entitled to a "continuing order for the cell phone company to provide stored records in the future."[72] Indeed, whereas two statutes permitting electronic surveillance ("ELSUR") to occur for a period of time subsequent to the execution of an authorizing order by a judicial officer, Title III and the Pen/Trap Statute, both contain time limits beyond which such surveillance cannot continue.[73] Section 2703 does not, thus strongly suggesting that it cannot rationally be viewed as a valid legal basis for "real time" ELSUR in the form of cell phone tracking. An exercise in comparing and contrasting is useful, conceded the USMJ, but only "as an effort to determine whether Congress 'intended' section 2703 to cover prospective cell site data."[74] Such intent is of no import, continued the court, because the "heart of the statute-granting authority [of § 2703] to obtain 'information' about cell phone customers—does not on its face contain any limitation regarding when such information may come into being."[75] In any event, the USMJ said, the government could get around this issue by submitting a request to the cell phone provider every hour (or more often) for "historical" records. "Thus, as a theoretical matter, the statute permits the Government to obtain cell site data on a continuing or ongoing basis even under a narrow reading of section 2703."[76]

Combining the Pen/Trap Statute with § 2703 makes eminent sense, the USMJ opined, because such a construct will contain the ELSUR time limitation that § 2703, by itself, lacks and because such a hybrid will avoid the difficulty foreseen—assuming just for the moment that the Pen/Trap Statute could be used alone—that it provides but a minimal proof standard (a mere certification of "relevance")[77] whereas § 2703 requires a higher evidentiary threshold, that of "specific and articulable facts" showing "reasonable grounds" exist to demonstrate that the

---

"portion of a tracking device" only if the phone were on and it were "pinged" by the service provider. *Id.* at 338.

72 *SDNY#1,* 405 F. Supp. 2d at 447.

73 Although extensions are permitted for cause shown, an initial court-ordered Title III has a duration of 30 days, 18 U.S.C. § 2518(5), and pens/traps can initially extend for up to 60 days, 18 U.S.C. § 3123 (c).

74 *SDNY#1,* 405 F. Supp. 2d at 447.

75 *Id.*

76 *Id.*

77 18 U.S.C. § 3122(b)(2).

requested information will prove "relevant and material" to the government's investigation.[78]

A stricter Fourth Amendment standard is not required, reasoned the court, because in the facts before it, the degree of location information sought was not pinpoint accuracy and thus was insufficiently precise to determine a person's situs inside a building. "These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart in urban areas. Moreover, the data is provided only in the event the user happens to make or receive a telephone call."[79] Additionally, the cell phone customer, by use of the cell phone, of necessity communicates information to a third party—the carrier. The Supreme Court has already instructed that such communication to a third party removes any possible privacy interest from the Fourth Amendment's ambit.[80]

By way of conclusion, the USMJ observed that because technology is changing rapidly, any cell site information order that it may issue in the future will set out with particularity what data that cell phone service companies may provide (and no other). This will be:

> (1) information regarding cell site location that consists of the tower receiving transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and (3) information that is transmitted from the provider to the government.[81]

F. Eastern District of Wisconsin – January 2006 (EDWIS)

In the Eastern District of Wisconsin case, based upon both the Pen/Trap Statute and 18 U.S.C. § 2703, the hybrid theory, the government sought an order directing the carrier to provide for a 60-day period subsequent to the date of any order:

> a. Originating and terminating cellular tower and sector information for all calls to and from [the target] cellular telephone (i.e., cell site activations);

---

78 *Id.* § 2703(d).
79 *SDNY#1*, 405 F. Supp. 2d at 449.
80 *Id.* (citing Smith v. Maryland, 442 U.S. 735, 744 (1979)).
81 *Id.* at 450.

> b. Map of cellular tower locations/addresses, sectors and orientations; and
> c. The physical address/location of all cellular towers in the applicable markets.[82]

Aware of the *SDTX#1, EDNY, DMD#1, DDC#3*, and *SDNY#1* decisions, the USMJ—troubled by the government's request for prospective (as opposed to historical) information—denied the application. The court did concede that the information here requested by the government was less invasive than that sought in *SDTX#1* and *EDNY* and, in fact, it was on par with that desired in *SDNY#1*. However, at the end of the day the USMJ could find no lasting virtue in the hybrid theory. Although it independently conducted its own legal analysis, the USMJ ultimately parted ways with the *SDNY#1* decision and found the *DDC#3* analysis to be the more compelling.

But the USMJ agreed with the *SDNY#1* USMJ to the extent the latter concluded that "cell site data, i.e., information on the location of cell site towers used by a cellular telephone, is included in the term 'signaling information' for purposes of the Pen/Trap Statute."[83] However, the CALEA caveat at 47 U.S.C. § 1002(a)(2) that "information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . [i.e.,] call identifying information[,] shall not include any information that may disclose the physical location of the subscriber . . . ." proved insurmountable and could not be overcome by trying to marry § 2703 with the Pen/Trap Statute.[84] As a result, the USMJ departed from the SDNY#1 opinion at that point.[85]

Just as the *DDC#3* USMJ did, the *EDWIS* court found the CALEA congressional testimony of FBI Director Freeh to be most telling and indicative of congressional intent:[86]

> . . . what is abundantly clear from . . . Director Freeh's testimony is that the language which found its way into the law was predicated on the Director's assertion to Congress that, in the government's view, pen register and trap and trace devices were not to be, and would

---

82 EDWIS#1, 412 F. Supp. 2d 947, 948-49 (E.D. Wis. 2006).
83 *Id.* at 953.
84 *Id.* at 956.
85 *Id.* at 955.
86 *See, e.g., id.* at 955-56.

> not be, used to secure location information for the cellular phone user.[87]

Even though the information sought here by the government was less comprehensive than that at issue in the *DDC#3* opinion, the *EDWIS* USMJ was unpersuaded that this was a meaningful distinction.

> [T]he government is only seeking the location(s) of the cell towers being used by the cell phone at the commencement and termination of calls. But, even such less precise location information was included in the 'tracking information' about which Congress was concerned and to which Director Freeh's mollifying remarks were directed.[88]

Finally, the court opined that § 2703 could not be used to bootstrap the Pen/Trap Statute. The USMJ remarked that "Director Freeh assured Congress that the legislation about which he was testifying and urging Congress to pass had nothing to do with, and did not relate to, the SCA, to wit, 18 U.S.C. § 2701, *et seq*."[89] Unfortunately for the government, the

---

87 *Id.* at 956. One segment from Director Freeh's testimony quoted by the USMJ allowed that

> [s]ome cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from 'true' tracking devices, which can require a warrant or court order when used to track within *a private location not open to public view*.

Id. (citations omitted; emphasis added). The emphasized language is key and its significance appears to have been overlooked by the USMJs who have focused upon it but generally. Taken together, *Knotts* and *Karo, see infra* text accompanying notes 230-44, teach that a tracking order predicated upon the Fourth Amendment is required *only* when information regarding what transpires *within* a residence (or curtilage not open to public view) is to be obtained—if, in fact, such discriminating tracking is even possible. As *Knotts* and *Karo* demonstrate, most subjects being tracked by law enforcement are out and about where they *could* be observed by the public and law enforcement. But do the Fourth Amendment, Rule 41, the SCA, or the Pen/Trap Statute even apply (or are they needed) in such situations? Prior to ECPA's enactment (and of the Pen/Trap Statute within it), the DOJ would obtain pen register orders based upon Rule 57(b) and the All Writs Act, 28 U.S.C. § 1651. Much like one's whereabouts on the public thoroughfares, there is no reasonable expectation of privacy with respect to the digits one dials from one's phone which one thus conveys to a third party. *See generally* Smith v. Maryland, 442 U.S. 735 (1979); United States v. N.Y. Tel. Co., 434 U.S. 159 (1977); *In re* the Application of U.S.A. for an Order Directing X to Provide Access to Videotapes, No. 03-89, 2003 WL 22053105 (D. Md. Aug. 22, 2003); United States v. Mosko, 654 F. Supp. 402 (D. Colo. 1987).

88 *EDWIS#1,* 412 F. Supp. 2d at 957.

89 *Id.* at 958.

USMJ found its hybrid theory to be "much more a legislative collage than a legislative mosaic."[90]

G. Western District of Louisiana – January 2006 (WDLA)

Because the government in *WDLA* sought only the same kinds and degrees of information at issue in *SDNY#1*, the substance and rationale of that decision were embraced by the *WDLA* USMJ. Specifically, the *SDNY#1* order

> did not authorize[ ] any cell site information that might be available when the user's cell phone was turned 'on' but a call was *not* in progress. . . . [As a result, the *WDLA* USMJ] adopt[ed] [the *SDNY#1* USMJ's] detailed analysis and will allow the Government to obtain the same information *subject to the same limitations*.[91]

Also noteworthy was that unlike the situation presented with a "true 'tracking device'"—which cannot be disabled or turned off by the target—the court observed that a cell phone user can prevent anyone from obtaining the tracking information the instrument is generating by either powering off the phone or simply by not making any calls.[92] Further, said the court, "[u]nlike true tracking devices, locations within buildings cannot be determined by the information authorized by this ruling."[93] In any event, because the location information actually being sought by the government in the case before him was relatively inexact (it will "not permit detailed tracking of a cell phone user within any residence or building") such that "[t]he Government will know only that the user has made or received a call on his cell phone, and that his cell phone communicated with a particular tower or towers during the call[,] . . . no Fourth Amendment concerns are implicated."[94]

---

[90] *Id.* "If Congress intended to allow prospective cell site information to be obtained by means of the combined authority of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the statutes themselves." *Id.*

[91] WDLA, 411 F. Supp. 2d 678, 680 (W.D. La. 2006) (emphasis added). The USMJ parenthetically remarked that the phones of some cell service providers, such as Nextel, are GPS-enabled which allows Nextel "to determine its users' locations anytime the cell phone is turned on." *Id.* at 681. Such authority was not sought here.

[92] *Id.*

[93] *Id.* at 682. It is questionable whether so-called "true" tracking devices can, from the outside, ascertain where in a building the transmitting device is situated.

[94] *Id.*

H. Western District of New York – February 2006 (WDNY)

Trying to build upon the *SDNY#1* and *WDLA* decisions, the government tried its hybrid or "convergence" theory yet again, this time in the Western District of New York, where it sought a court order from a USMJ for relatively imprecise cell phone location information. It asked for "cell site tower location information . . . at the inception and termination of a call made and received by an identified cellular telephone."[95] Such, the DOJ argued, would only provide the "general vicinity" and not a specific location for a phone.[96] The USMJ, well aware of all of the preceding USMJ decisions discussed above, ultimately fell in line with the majority.

First, however, the USMJ acknowledged those portions of DOJ's hybrid/convergence argument that he found correct: (1) "signaling information," which—post USA PATRIOT Act[97]—an authorized pen register may obtain, includes "cell site location data"; (2) a pen register is permitted to "capture[ ]" such data upon the government's certification that the "information likely to be obtained is relevant to an ongoing criminal investigation"; (3) the SCA enables the government to secure *historical* cell site data upon a demonstration of "reasonable grounds to believe" that the information to be obtained is "relevant and material to an ongoing criminal investigation"; but that (4) CALEA prohibits the government from getting the very information it seeks pursuant to the Pen/Trap Statute's "likely to be relevant standard[.]"[98]

Then the USMJ turned to the shortcomings in DOJ's argument, finding the "government's 'convergence' argument unconvincing[,]" and found nothing in the express language of the Pen/Trap Statute, CALEA, or the ECPA that indicates judges should follow a theory converging the statutes.[99] That Congress even envisioned such a unorthodox, tortured

---

95 WDNY, 415 F. Supp. 2d 211, 212 (W.D.N.Y. 2006). Assisting the court in its understanding of the technology involved was a letter appended to the government's pleadings from the "Court Order Compliance Manager" of cell phone provider Verizon. *Id*. at 213 n.3. The degree of cell phone location information here being sought by DOJ would not make it possible to "pinpoint the exact location of the mobile phone" because, in part, Verizon's "ability to provide a cell phone's location 'can range from several hundred meters to several miles.'" *Id.*

96 *Id.* at 212.

97 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

98 *WDNY*, 415 F. Supp. 2d at 214 (internal citations omitted).

99 *Id.* Continuing, the USMJ added,

matrimony of three disparate laws, the USMJ felt, was beyond the pale. He shared the concerns expressed by the majority of the Magistrate Judges—who had already considered the issue now before him "as to the wisdom and logic of predicating Congress's intent to combine statutory provisions separately enacted over a fifteen year period to create a new and independent hybrid authorization mechanism on the use of the word 'solely' in the [CALEA] exception clause."[100]

Additionally, that the government had here limited its request to generalized (as opposed to equally available precise) cell phone location information was of no import.

> [T]here is nothing in the legislative history of CALEA to suggest that the exception clause was intended by Congress to create some sort of sliding scale pairing mechanism, with the evidentiary standard for ordering disclosure hinging on the type or duration of pen register data or signaling information sought by law enforcement.[101]

If the Pen/Trap Statute, CALEA, and the SCA are to be converged, such intent should come from Congressional direction as opposed to DOJ supposition: "The government's concerns over the 'ambiguity of the statutes' are well founded, but it is the Congress and not the Department of Justice who is empowered to respond to those concerns."[102] Concluding, the USMJ wrote that as that statutory framework now existed, prospective cell phone location information could only be obtained upon the basis of an application grounded upon probable cause.[103]

> [I]f Congress wanted judges to grant disclosure of real time cell site data by importing the procedural rules and safeguards of a statute that Congress directed *not* be used to authorize the disclosure of prospective cell site location data (the Pen Register statute) into a statute and under a standard that Congress specifically reserved for the production of *historical* telephone records (the SCA), Congress could have and would have clearly said so. Congress did not.

Id. at 214-15.

100 *Id.* at 215. Recall that the "exception clause" is 47 U.S.C. § 1002(a)(2)(B).

101 *WDNY*, 415 F. Supp. 2d at 219. The logic of this argument does much to undermine the theses underlying the *SDNY#1* and *WDLA* decisions.

102 *Id.*

103 "The Court does not agree with the government that it should impute to Congress the intent to 'converge' the provisions of the Pen Statute, the SCA and CALEA to create a vehicle for disclosure of prospective cell location information on a real time basis on less

I. Southern District of West Virginia – February 2006 (SDWVA)

Given the facts in the decision out of the Southern District of West Virginia, the USMJ did not directly address the issue of what, if any, statutes—alone or in combination—authorize federal law enforcement agencies ("LEAs") to acquire real-time location information of a cell phone subscriber notwithstanding that the DOJ had specifically invoked both the Pen/Trap Statute and § 2703 in support of its application.[104] Here, the U.S. Marshals Service ("USMS") was trying to locate a fugitive who was using someone else's cell phone.[105] Thus, the fugitive was not the paying customer of the cell phone service of investigative interest—a fact the USMJ found determinative.[106]

Additionally, the USMJ gratuitously remarked that she was mindful of all the earlier published opinions written by her USMJ colleagues on the score and, like the majority of them, she was "unpersuaded by the government's argument that Chapters 206[107] and 121[108] [of Title 18, U.S.C.], considered together, permit a court to authorize use of a pen register and trap and trace device in order to locate a *subscriber* using a cell phone in a geographical area, despite the provisions of 47 U.S.C. § 1002(a)(1)."[109] It was unnecessary, however, for her to specifically rule on the matter in order to dispose of the case because only a subscriber (who can also be a user), and not a mere user, i.e., one who is not also a

---

than probable cause." *Id.* The court parenthetically noted that at least one bill, S. 2130, 109th Cong. (2006), sought to clarify the evidentiary standard necessary to obtain real time/prospective cell phone location information. *Id.* at 219 n.6. Senate Bill 2130 would require a Title III application—certainly a probable cause requirement—to obtain cell site data. Also taking note of this bill, the *SDNY#2* USMJ opined that "[i]f the Department of Justice needs to obtain *prospective* cell site location information in criminal investigations, it needs to ask Congress to explicitly grant it such authority." SDNY#2, No. 06 CRIM. MISC. 01, 2006 WL 468300, at *2 (S.D.N.Y. Feb. 28, 2006).

104 More particularly, the application before the USMJ sought

> the use of a pen register which would capture and report at the same time, originating and terminating 'Cell Site Location Information,' which is defined as information which identifies the antenna tower receiving transmissions from that cell phone (and any information on what portion of that tower is receiving a transmission, if available) at the beginning and end of a particular telephone call made or received by the cell phone's user . . . .

SDWVA, 415 F. Supp. 2d 663, 664 (S.D. W. Va. 2006).

105 *Id.*

106 *Id.* at 666.

107 18 U.S.C. §§ 3121-3127 (2000).

108 18 U.S.C. §§ 2701-2712 (2000).

109 *SDWVA*, 415 F. Supp. 2d at 665.

subscriber, is protected under 47 U.S.C. § 1002(a)(1).[110] As a result, the USMJ granted the government's application—certainly based upon less than probable cause—requiring the cell phone carrier to provide it with "Cell Site Location information for all calls made to or from the subject telephone for a period of sixty days from the date of [the court's] Order, or until the arrest of the subject fugitive, whichever comes first."[111]

J. Disrict of Maryland – February 2006 (DMD#2)

Three months after the government was denied an order for "real time cell site information' . . . whenever the phone was on," the same USMJ was asked for an order directing a wireless service provider to surrender "cell site information concerning the physical location of antenna towers associated with the beginning and termination of calls to and from the subject cellular telephone."[112] Borrowing from both § 2703(d) and the Pen/Trap Statute (the hybrid theory), the government "proffered 'specific and articulable facts'" demonstrating that there were "'reasonable grounds' to believe that" the information to be obtained would be both "relevant and material" to its ongoing investigation.[113] The court was as unimpressed with the government's cobbled together approach this time as it was the last:

> the court DENIES the government's request because the proffered statutory authority is insufficient. Unless and until Congress takes further action, the court may only authorize disclosure of prospective cell site information upon a showing of probable cause pursuant to Rule 41.[114]

The government protested that this application was different in three particulars from the first: (1) it was now seeking location information only at the inception and termination of calls, i.e., not also during the course of them; (2) it now wanted to know the location of only one cell tower "with which the target phone is communicating"; and (3) it sought only the location information "stored" by the carrier.[115] The government's attempt at differentiation was misplaced, countered the

---

110 *Id.* at 666.

111 *Id.*

112 DMD#2, 416 F. Supp. 2d 390, 391 (D. Md. 2006) (internal quotations omitted).

113 *Id.*

114 *Id.* The USMJ allowed that instead of using Rule 41, the government could also avail itself of the more stringent Title III standard. *Id.* at 391 n.1.

115 *Id.* at 392.

court, because the "earlier decision was not based on constitutional grounds but on the lack of statutory authority . . . ."[116] The court did, however, rethink one aspect of its previous opinion and accepted "the government's contention that a mechanism that transmits cell site information to the government falls within the definition of a pen register in 18 U.S.C. § 3127(3) [because] . . . .[c]ell site information is 'signaling information' as discussed by [the Pen/Trap] statute[ ]."[117] However, just because the CALEA segment at 47 U.S.C. § 1002(a)(2) precludes the *sole* use of the Pen/Trap Statute to secure such "signaling information," does not mean the USMJ bought into the government's hybrid argument:

> [T]he court pauses before concluding, based on the single word 'solely,' that Congress intended [CALEA] § 103(a)(2)[118] to affirmatively authorize disclosure of cell site information on a prospective basis through any combination involving the Pen/Trap Statute. An equally valid interpretation of the 'solely' phrase is that Congress intended that authority to locate subscribers should derive largely, if not wholly, elsewhere. At best, Congress was discouraging, not encouraging, reliance on the Pen/Trap Statute for this purpose.[119]

Assuming *arguendo* that Congress intended that the Pen/Trap Statute be used in conjunction with a second law in order that prospective cell phone location information could be obtained, the court said, that additional statute certainly could not be § 2703.[120] "First, the SCA simply is not and never was intended to be a statute that authorizes prospective surveillance . . . . Second, § 103(a)(2) of CALEA was predicated on Director Freeh's assertion that the SCA and the Pen/Trap Statute were distinct."[121] At the end of the day, concluded the USMJ, the government's hybrid theory "is at best murky and, at worst, illusory."[122]

---

116 *Id.*

117 *Id.* at 393-94.

118 Codified at 47 U.S.C. § 1002(a)(2) (2000).

119 *DMD#2,* 416 F. Supp. 2d at 394-95.

120 *Id.* at 395.

121 *Id.* "The SCA regulates access to records and communications in storage and therefore lacks provisions typical of prospective surveillance statutes[ ]" such as set time periods after which electronic surveillance must cease (absent renewal), reporting requirements, and prescribed sealing requirements. *Id.* at 395 n.7.

122 *Id.* at 396.

K. Southern District of New York – February 2006 (SDNY#2)

The USMJ who authored this opinion was completely at odds with his colleague who wrote *SDNY#1,* thus setting up a split of authority within the same federal judicial district.[123] Basing its application upon § 2703(d), the government specifically sought authority to use a pen register to

> capture and report at the same time originating and terminating cell site location information (specifically, information which identifies the antenna tower receiving transmissions from that cellphone (and any information on what portion of that tower is receiving a transmission, if available) at the beginning and end of a particular telephone call made or received by the cellphone's user, which information is to be transmitted from the cellphone's service provider to the DEA and other law enforcement agencies)[.][124]

In denying the government's application without reservation, the USMJ parenthetically observed that prospective cell site location information had been the frequent topic of USMJs both in the circuit and around the country, but that even though a fellow USMJ in the Southern District of New York had approved a comparable application by the government, this USMJ came to the opposite conclusion.[125] In siding with the majority of USMJs who opined previously on the matter, the USMJ saw little need to rephrase those opinions or, in his words, to "reinvent the wheel,"[126] but at the same time, he wanted to clearly set forth his understanding of that "majority" position. He emphasized his agreement with the prior cases that had rejected the "'hybrid' statututory interpetation theory," and thus declined to permit a combination of CALEA, the SCA, and the Pen/Trap Statute to obtain "prospective cell site location information."[127]

---

123 Continuing, the USMJ observed that in so deciding he joined "eight decisions by seven other Magistrate Judges (including [two] Magistrate Judges in this Circuit) in concluding that statutory authority for prospective cell site location information is lacking." SDNY#2, No. 06 CRIM. MISC. 01, 2006 WL 468300, at *1 (S.D.N.Y. Feb. 28, 2006) (citations omitted).

124 *Id.*

125 *Id.*

126 *Id.* at *2.

127 *Id.*

If the DOJ wants authority to obtain prospective cell site location information based upon a less than probable cause standard, the court concluded, it would be necessary to seek it from Congress. Addressing the now-existing split within the Southern District of New York regarding cell phone tracking, the USMJ urged the government to file "timely objections to this Opinion with a Part I[128] District Judge or otherwise seeking appropriate review by an appropriate District Judge."[129]

L. Eastern District of California – March 2006 (EDCA)

In *EDCA*, the USAO sought information from a wireless service provider that would be "expected to identify the specific cell tower(s) 'handling' the initiation, reception or maintenance of phone calls associated with the specified cell phone."[130] Given recent precedent, the USMJ surprisingly granted the government's application "in all particulars" by "proper[ly] adhering to established rules of statutory construction[.]"[131] The government's hybrid theory—combining § 2703 with the Pen/Trap Statute—was and is a perfectly reasonable work-around addressing CALEA's admonition that the Pen/Trap Statute cannot be the "sole" statutory basis by which to obtain a cell phone subscriber's physical location. Indeed, the USMJ castigated his colleagues who penned the earlier decisions, accusing them of

> using their "intuition" and going behind the plain meaning of an otherwise unambiguous statutory text in their use of legislative history . . . [to] conclude[ ] that only a warrant issued on probable cause or perhaps a wiretap application, 18 U.S.C. § 2510 aka "Title III," will do for obtaining cell site location information.[132]

The USMJ did, however, go out of his way to limit the scope of his order to that cell phone location information generated during the course of an actual wireless call. In other words, the authorization provided

---

128 *See generally* N.Y. R. USDCTSD DIV. BUS. R. 3, a portion of which states that "[p]art I is established for hearing and determining certain emergency and miscellaneous matters in civil and criminal cases and for processing criminal actions and proceedings through the pleading stage. Judges shall choose assignment to Part I from an appropriate schedule . . . ." *Id.*

129 *SDNY#2*, 2006 WL 4688300, at *2.

130 EDCA, No.S-06-SW-0041, at *1 (E.D. Cal. Mar. 15, 2006).

131 *Id.* at *2.

132 *Id.* at *4. "Legislative history cannot be utilized to create ambiguity in an otherwise unambiguous text." *Id.* at *5.

would not also extend to location information available at times when the phone, although turned on and registering, was not being used at the moment to make or receive a communication.

> While it is reasonable to think of roaming signals from a cell phone which is merely operative as signaling information, Congress has indicated that it desires to limit the acquisition of signaling information more narrowly to require a communication[ ] . . . [which] bespeaks the imparting of information by or between persons via electronic means, not the mere, constant contact of one machine with another machine.[133]

M. Southern Disrict of Texas – April 2006 (SDTX#2)

In this cell site tracking decision, the first by a U.S. District Judge, the court allied itself with the reasoning in the three earlier decisions granting the government limited relief because

> in the present case the government has included significant limits on the authorization it seeks. The government is *not* seeking: (1) to activate remotely the subject telephone's GPS functionality; (2) to obtain information from multiple cellular antenna towers simultaneously to 'triangulate' the precise location of a cell phone; or (3) to place calls to a particular cell phone repeatedly or otherwise track on a continuous basis the location of a cell phone when no call is being placed or received.[134]

According to the court, the government here sought permission to *install* a pen/trap device (as opposed to commanding a cell phone provider to produce pen/trap information) in order to obtain "cell-site information at the origin and termination of calls and, if reasonably available, during the progress of a call that is not initiated by the government itself."[135] Concluding that the government was only a little

---

133 *Id.* at *7 (citing 47 U.S.C. § 1001(2) (2000)). "Thus, a valid order permitting the acquisition of signaling information refers only to the information generated by a phone call, i.e., a communication." *Id.*

134 SDTX#2, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006).

135 *Id.*

bit pregnant, the court opined that the government "met its statutory burden under 18 U.S.C. § 3121 *et seq.* and § 2703(d)."[136]

N. Southern District of Indiana – June 2006 (SDIND)

This decision differs from all the others discussed in this article because here the U.S. District Judge ruled—after the cell site location information had been obtained—upon a defendant's motion to suppress the data received from a carrier pursuant to a USMJ order. This contrasts with the other opinions covered in that they discuss whether, in the first instance, an order directing a carrier to provide cell site location information should even be entered. Here the tracking information had been prospectively obtained following entry of a USMJ's 60-day order in response to the government's pleading, the latter having been based upon 18 U.S.C. §§ 2703(c)(1)(B)(ii), 2703(d), 3124, or some combination thereof.[137] Based upon cell site location data obtained from the carrier along with other cell phone location information gathered with a deliberately unspecified government electronic device, DEA, and the U.S. Marshals service determined that a phone belonging to an indicted fugitive was located in a Chicago multi-unit dwelling.

The defendant raised the argument[138] that "receipt of cellular site information" as the result of the USMJ's order approving of the government's hybrid theory "exceeded the limitations imposed by those statutes [Pen/Trap and SCA] in permitting a cell phone to become a tracking device."[139] Also, argued the defendant, any order permitting acquisition of cell phone location information must be grounded upon probable cause and not upon "specific and articulable facts."[140] The court concluded that neither the SCA nor the Pen/Trap Statute

---

136 *Id.*

137 The text of the order, not a paragon of clarity, seems to indicate such. SDIND, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *1 n.5 (S.D. Ind. June 30, 2006); *see also id.* at *6 (indicating the government proceeded using its "hybrid" theory). However, footnote 15 states that the order to obtain cell site location information from the carrier for 60 days was predicated upon 18 U.S.C. § 2703(d). *Id.* at *6 n.15. Note that the government secured the arrest not only by relying only upon cell site location information received from a cell phone service provider but from information received from one of the government's own cell phone tracking devices. *Id.* at *1 n.1.

138 *Id.* at *6. It is sometimes difficult to discern whether the court is addressing issues surrounding acquisition of cell phone location information from the carrier or from the government's electronic device.

139 *Id.*

140 *Id.*

"cover[ed] real time cell site information[.]"[141] In finding the SCA inapplicable, the court came to the now familiar conclusion that "real time cell site information is not a 'stored communication' or record and therefore is not covered by [18 U.S.C.] § 2703(c). Further, the title of the section itself suggests that cell site information is not included."[142] Additionally, the court concluded that the Pen/Trap Statute could not apply to prospective cell site location information because of the CALEA exception.[143] Its position eroding, the government countered that even if the SCA and the Pen/Trap Statute did not provide a basis upon which to undergird the order, neither did those statutes provide suppression as a remedy. The court concurred: "We agree that the statutory language in the Pen/Trap Act and the SCA does not mandate exclusion of such evidence as the sanction for violations of those requirements, and in fact, the [SCA] expressly rules out exclusion as a remedy."[144]

If the government's hybrid theory does not provide a basis for the accumulation of real-time cell site location information, what does?

---

[141] *Id.* at *7. Parenthetically, and somewhat bizarrely, the court said that Title I of ECPA, Pub. L. No. 99-508, 100 Stat. 1848 (1986), consisted of "provisions governing tracking devices." *SDIND*, 2006 WL 3197181, at *7. Of the eleven sections in Title I, only one—section 108—dealt with tracking devices. The purpose of section 108 was to add § 3117, *Mobile tracking devices*, to Title 18, U.S. Code. Section 3117(a) (2000), which provides that if a tracking device installation warrant or order is issued in one judicial district, it may be monitored in all districts. Section 3117(b), does nothing more than provide a bland, unremarkable definition of "tracking device" which is said to be "an electronic or mechanical device which permits the tracking of the movement of a person or object." To suggest, therefore, that Title I is chock-full of tracking device provisions is to miss the mark. In fact, the great bulk of ECPA's Title I makes changes to Title III, Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (1968), the latter having originally been enacted in 1968.

[142] *Id.* The court accurately points out the "structural differences" between statutes relating to the acquisition of historical records and those dealing with the collection of data to be created in the future "suggest" the conclusion that "Congress did not intend the SCA to cover real time tracking of a cell phone." *SDIND*, 2006 WL 3197181, at *7 n.20.

> 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.

Id.

[143] *Id.* at *8.

[144] *Id.* (citing 18 U.S.C. § 2708 (2000), *Exclusivity of remedies*, part of the SCA, which provides that "The remedies and sanctions described in this chapter [i.e., 18 U.S.C. § 2701-2712] are the only judicial remedies and sanctions for nonconstitutional violations of the chapter.").

> Because the ECPA was not intended to affect the legal standard for the issuance of orders authorizing these devices [tracking devices], a Rule 41 probable cause showing and procedures were (and still are) the standard procedure to authorize the *installation* . . . of mobile tracking devices.[145]

But a Rule 41/Fourth Amendment violation could occur in the case of cell phone tracking only if there were a warrantless search. "In other words, only if a Fourth Amendment privacy interest exists which would be violated by the government's mobile tracking of a cell phone, is a warrant necessary for the search."[146] Researching the law in the Seventh Circuit, the court could find no "binding precedent" which would inform it whether a Rule 41 probable cause warrant were needed "before the government can use cell site information to track a cell phone's location."[147] Relatedly the court could neither find any guidance concerning whether a defendant has a suppression remedy if the government fails to obtain a Rule 41 warrant to obtain cell site location information.[148] The court opinions which exist on the score, discussed in this Article, "are procedurally distinguishable in that the issue arose there when the government requested receipt of cell site information in a warrant application[.]"[149] In any event, the court concluded "that no statutory basis exists for suppression of the evidence[ ]"[150] which left upright only a Fourth Amendment analysis.

Basing his argument on *Kyllo v. United States*,[151] the defendant next raised the compelling argument that because the tracking at issue "intruded into his private dwelling [his apartment], as opposed to a public place," the warrantless gathering of cell site location information constituted a Fourth Amendment violation.[152] The court rejected this contention, concluding that,

> in *Kyllo*, law enforcement targeted the home to gain information relating to activities underway inside. Here,

---

145 *Id.* at *10 (internal citations omitted; emphasis added).

146 *Id.* The court added that "[t]he warrantless *monitoring* of a tracking device located in a public place generally does not implicate the Fourth Amendment." *Id.* at *8 n.25 (citations omitted; emphasis added).

147 *Id.* at *10.

148 *Id.*

149 *Id.*

150 *Id.* at *11.

151 533 U.S. 27 (2001).

152 *SDIND*, 2006 WL 3197181, at **11-12.

> law enforcement officers targeted a particular phone only as to its location . . . . [The law enforcement officer] did not obtain any information regarding [the defendant's] home, beyond the fact that the target phone was present in one of the three apartment units at [the street address.][153]

Additionally, and no doubt drawing upon *United States v. Miller*,[154] the court concluded that the defendant brought law enforcement scrutiny on himself by leaving his cell phone on, which "knowingly exposed" his signaling information "to a third-party, to wit, the cell phone company."[155]

O. Northern District of Indiana – July 2006 (NDIND)

In a 2006 case out of the Northern District of Indiana, the government appealed the denial of a cell site location application which had been grounded upon the Pen/Trap-SCA hybrid theory, but the U.S. District Judge upheld the USMJ to whom the pleading was initially presented. Sought were both historical and "real time" location information. "Either way," the court said, "the Government is requesting an order requiring cellular phone companies to identify the specific cell tower from which a call originates, is maintained, or received for an incoming or outgoing call . . . . [S]uch information is unobtainable absent a warrant."[156] Recalling that one thrust of CALEA was to ensure that pen/traps could not be used to secure cell phone location information, the court noted that the earlier decisions rejecting the government's hybrid theory did so because the purpose of the government's cell site location information request "is to accomplish what Congress attempted to avoid, that is, permitting law enforcement to track individuals using cell location information."[157] The court, like many of the others before it, also examined (then) FBI Director Freeh's congressional ELSUR testimony and quoted with approval the *EDWIS#1* USMJ who said that it made absolutely "no sense" to him "that, by use of the word 'solely' in 47 U.S.C. § 1002(a)(2), Congress was in some back-handed fashion intending to allow the SCA to be used in conjunction

---

153 *Id.* at *13.

154 United States v. Miller, 425 U.S. 435 (1976); *see infra* note 294 and accompanying text.

155 *SDIND*, 2006 WL 3197181, at *13. "Though the signal originated from within [the defendant's] residence, it was capable of being monitored outside the home." *Id.* The final nail in the defendant's coffin was his lack of standing because the phone that was tracked to his apartment belonged to someone else.

156 NDIND, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, at *1 (N.D. Ind. July 5, 2006).

157 *Id.* at *4.

with the Pen [Register] Statute to obtain the very information that Director Freeh assured Congress he was not seeking authority to obtain under the proposed legislation."[158] As a result, the court endorsed the conclusion reached by the *NDIND* USMJ that

> (1) the Government cannot rely on the Pen Register Statute to obtain cell site location information; and (2) converging the Pen Register Statute with the SCA in an attempt to circumvent the exception in CALEA is contrary to Congress' intent to protect cell site location information from utilization as a tracking tool absent probable cause under the Fourth Amendment.[159]

In the course of further explaining its denial of the government's application, the court again turned to the *EDWIS#1* opinion, upon which it heavily relied, where it was observed that any evidence of congressional intent to allow the combined authority of the SCA and the Pen Register Statute to provide the basis for obtaining cell site information was missing from the statutes.[160]

P. Southern District of Texas – July 2006 (SDTX#3)

In light of the *SDTX#2* opinion by a U.S. District Judge, and because the government now limited the scope of its cell site location information request, USMJ Smith (the author of *SDTX#1*) again considered a government Pen/Trap-SCA hybrid application.[161] The USMJ emphasized that "[n]o published court opinion has yet agreed with the government that *unlimited* cell site information is obtainable via the combined authority of the Pen/Trap Statute, CALEA, and the SCA."[162]

That said, and believing that *SDNY#1* was the best opinion so far which championed the government's hybrid approach, in again denying the government's application, USMJ Smith proceeded to take on *SDNY#1* directly. The government's statutory convergence theory, he said, first proceeded from the belief that the Pen/Trap Statute is the

---

158 *Id.* at **12-13 (quoting EDWIS#1, 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006)).

159 *Id.*

160 *Id.* at *5 (quoting *EDWIS#1*, 412 F. Supp. 2d at 958).

161 "Invoking the same legal theory rejected by this court last fall, the Government again seeks to obtain an order authorizing access to prospective cell site information as part of a criminal investigation." *Id.* The court unflatteringly referred to the Government's hybrid theory as a "three-rail bank shot." SDTX#3, 441 F. Supp. 2d 816, 828 (S.D. Tex. 2006) (quoting SDTX#1, 396 F. Supp. 2d 747, 765 (S.D. Tex 2005)).

162 *SDTX#3,* 441 F. Supp. 2d at 827.

"*exclusive* mechanism" by which cell phone "signaling" information could be obtained.[163] The USMJ dismissed this contention, saying that of necessity it results in the illogical conclusion that "a judge who would be compelled to grant a pen register application solely upon the Government's certification of relevance must deny that application if the Government goes further and establishes probable cause under Rule 41."[164] In fact, one court had already determined that such a conclusion was "absurd."[165] In particular, the "[l]egal process is calibrated to the degree of intrusion. So 'the greater the privacy interest at stake, the higher the threshold Congress uses.'"[166] Further the USMJ explained, the Supreme Court had already specifically ruled in *United States v. New York Telephone Co.*[167] that pen register authorization could be secured with a warrant satisfying Rule 41.[168]

The second peg upon which the government's hybrid theory rested is the conclusion that CALEA's "solely pursuant" caveat mandates the addition of a second, not-inconsistent grant of statutory authority—such as the SCA—which, when paired with the Pen/Trap Statute, will permit the acquisition of cell site location information. However, "CALEA legislative history contains no clue that its drafters imbued the word 'solely' with the significance now attributed by hybrid proponents."[169] Further, "[t]he 'solely pursuant' phrase leaves open the possibility that a pen/trap order may be neither necessary nor sufficient to obtain such [cell site location] data . . . [It] may be one route, but not the only route, to obtain cell site [location] information."[170]

The third prong of the hybrid theory incorporates the SCA. But that statute "expressly prohibits a phone company from disclosing subscriber information 'to any governmental entity,' except under certain carefully delineated circumstances[,]"[171] and of the six exceptions, not one mentions a conjoining with the Pen/Trap Statute. "In fact, the sixth

---

163 *Id.*

164 *Id.*

165 *Id.* (citing DMD#2, 416 F. Supp. 2d 390, 397 n.11 (D. Md. 2006)).

166 *Id.* at 829.

167 *See* United States v. N.Y. Tel. Co., 434 U.S. 159 (1977).

168 "In support of its Rule 41 holding, the Court twice invoked a variant of the 'greater includes the lesser' maxim: '[I]t would be anomalous to permit the recording of conversations by means of electronic surveillance while prohibiting the far lesser intrusion accomplished by pen registers.'" *SDTX#3*, 441 F. Supp. 2d at 830 (citing United States v. N.Y. Tel. Co., 434 U.S. 159, 170 (1977)).

169 *SDTX#3,* 441 F. Supp. 2d at 832.

170 *Id.* at 832-33; *see supra* note 35; *Alternative Legal Foundation, infra* Part III.A.

171 *SDTX#3,* 441 F. Supp. 2d at 834.

exception (authorizing disclosure 'to any person other than a governmental entity') underscores that the primary intent of the prohibition was to guard against unwarranted access to subscriber information *by the government*."[172] In sum, the USMJ concluded that the government's convergence or hybrid theory "self-destructs, its initial premise at war with its intended conclusion."[173]

Other factors also argue against the hybrid theory, to include "the temporal gaps among the relevant statutes: 15 years between the ECPA and the PATRIOT Act, 7 years between CALEA and the PATRIOT Act, and 4 years between the effective dates of CALEA's amendment of the SCA and the CALEA proviso[.]"[174] Coupled with this is the statement of CALEA's sponsor in the House describing the final bill as placing limitations on law enforcement's use of phones as *tracking devices*.[175] Finally, another detraction from the hybrid theory is that none of the opinions which have given it credence by permitting the acquisition of limited cell site location information directly tackled the 18 U.S.C. § 3117(b) tracking device definition.[176]

Statutory infirmities aside, the hybrid theory also raises unsatisfactorily addressed constitutional issues. "If the dual [hybrid] theory were found to authorize the limited cell site data sought here, it must necessarily authorize far more detailed location information, such as triangulation and GPS data, which unquestionably implicate Fourth Amendment privacy rights."[177] In short, the USMJ held fast to his original opinion and looked askance at *SDTX#2*, the opinion by a U.S. District Judge which intervened between USMJ Smith's opinions in *SDTX#1* and *SDTX#3*.

Q. District of Maryland – July 2006 (DMD#3)

Notably this decision was authored by the USMJ who also wrote both *DMD#1* and *DMD#2*. The procedural history of the case is both unusual and interesting. The government sought prospective cell site location information for the purpose of apprehending a fugitive and it presented sufficient probable cause evidence to underpin a Rule 41

---

172 *Id.*

173 *Id.* at 835.

174 *Id.*

175 *Id.* (internal citation omitted; emphasis added by USMJ).

176 *Id.*

177 *Id.* at 837. One truly cannot be just a little bit pregnant: "The constitutional problems created by this [hybrid] interpretation of the electronic surveillance statutes are the same, regardless of the breadth of cell site data sought in a given case." *Id.*

search warrant. The USMJ advised the government that he would issue such a warrant upon submission of an affidavit, but the government declined to do so

> because it considered this a test case for its position that an order to obtain prospective cell site information can be entered upon less than probable cause pursuant to the combined authority of [the Pen/Trap statute and the 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." 18 U.S.C. § 2703(d).[178]

But, having twice rejected the government's hybrid theory before, the USMJ did not hesitate to reject it a third time.[179]

R. Eastern District of Wisconsin – October 2006 (EDWIS)

Choosing again to beat its head against the wall yet another time, the government relied upon its hybrid theory in seeking limited cell site location information[180] and lost before both the USMJ and the U.S. District Judge to whom subsequent appeal was made.[181] Framing the issue, the court noted "that the issue is not *whether* the government can

---

178 DMD#3, 439 F. Supp. 2d 456, 456-57 (D. Md. 2006).

179 "I have twice rejected this [hybrid] position, as have the majority of other courts to consider it. I advised the government that, without a sworn affidavit, I would deny its application for prospective cell site information, and, to the extent the application seeks such information, it is hereby DENIED." *Id.* at 457.

180 The government sought "the originating and terminating cellular tower, a map of tower locations, and the physical address of all cellular towers in the applicable market—commonly referred to as the J-Standard[.]" EDWIS#2, No. 06-MISC-004, 2006 WL 2871743, at *3 n.2 (E.D. Wis. Oct. 6, 2006). The court recognized the "little bit pregnant" posture of the government's request for limited cell site location information, noting that "nothing in its statutory argument would forbid it from obtaining triangulation information for the entire cell or even when the phone is simply on but not in use. . . . Indeed, courts have rejected similarly 'narrowed' requests." *Id*. But what is the "J-Standard?" After "extensive" discussions with the FBI, the J-Standard (J-STD-025) was established by the Telecommunications Industry Assn. ("TIA"), "an accredited standard-setting body[.] . . . [The J-standard], outlines the technical features, specifications, and protocols for carriers to make subscriber communications and call-identifying information available to law enforcement agencies having appropriate legal authorization." U.S. Telecomm. Ass'n v. FCC, 227 F.3d 450, 455 (D.C. Cir. 2000).

181 Oddly, at some point the government appears to have abandoned its hybrid theory in favor of a successful probable cause presentation before the USMJ. *EDWIS#2,* 2006 WL 2871743, at *3.

obtain cell cite [*sic*] information. Rather, the issue is the *standard* it must meet before a court will authorize such disclosure."[182] The court then began its opinion by providing a hierarchical overview of the relevant Federal statutes governing ELSUR: Title III, which the court dubbed a "super warrant[,]"[183] the SCA, which "imposes an 'intermediate' standard on the government[,]"[184] and the Pen/Trap Statute, which "requires the lowest quantum of information."[185] Completing that task, the court also threw in both 18 U.S.C. § 3117(b), which rather unhelpfully does nothing more than provide a definition of the term "tracking device," and CALEA, believing each was relevant to the issue at hand.

Inexplicably, and apparently incorrectly reading both *Knotts*[186] and *Karo*,[187] the court then *wrongly* stated that "to obtain such a [tracking] device, the government must meet the probable cause standard set forth in Fed. R. Crim. P. 41."[188] (As will be discussed below in Part III.A, *Alternative Legal Foundation*, probable cause is definitely not needed in all instances to install or monitor a tracking device.)[189] However, the court seems to correct itself by citing both *Knotts* and *Karo* before concluding that "[i]t is doubtful that the government's use of cell site information to track a suspect implicates the *Fourth Amendment*, requiring use of the probable cause standard as a constitutional matter."[190]

The court summarized the Government's hybrid argument as one which contends that "the Pen/Trap statute *must* be coupled with some other statute due to the restriction contained in CALEA."[191] The court was adamant that this conclusion "is simply wrong"[192] because "[a]s the Supreme Court has held, authorization of a greater intrusion [e.g., Title III, search warrant] necessarily authorizes a lesser intrusion [*e.g.*, pen register/trap and trace, cell site data]."[193] Thus "there is no reason to believe that CALEA *requires* the coupling of the Pen/Trap statute with the SCA or any other statute, as opposed to requiring the government to

182 *Id.* at *1.
183 *Id.* at *2 (internal citations omitted).
184 *Id.* (internal citations omitted).
185 *Id.*
186 *See* United States v. Knotts, 460 U.S. 276 (1983).
187 *See* United States v. Karo, 468 US 705 (1984).
188 *EDWIS*#2, 2006 WL 2871743, at *2.
189 *See infra* Part III.A.
190 *EDWIS*#2, 2006 WL 2871743, at *5 n.6.
191 *Id.* at *3 (emphasis added).
192 *Id.* at *4.
193 *Id.* at *4 nn.3-4 (internal citations omitted).

make its request under Rule 41 or [18 U.S.C.] § 2518."[194] The court then assessed whether the SCA, Rule 41, or 18 U.S.C. § 3117(b) was "the best source of authority for accessing telephone information."[195] Opting in favor of Rule 41, and despite the government's denial that cell site information is a "tracking device" under § 3117(b), the court determined that a Rule 41 probable cause warrant is "'the standard procedure for authorizing the installation and use of mobile tracking devices.'"[196]

Despite already having reached its conclusion that cell site location information, if it is to be had at all, should be obtained by Rule 41 in conjunction with 18 U.S.C. § 3117 or pursuant to Title III, the court nevertheless entered upon an extended discussion of why the government's hybrid theory is unpalatable. First, to the extent the SCA can be said to apply, cell site location information cannot come within its ambit because the statute relates to "electronic communication service" which in turn, provides users with the "ability to send or receive wire or electronic communications."[197] But a wire communication is one involving an "aural transfer,"[198] which cell site location information is not, and by its terms, an electronic communication does not include "any communication from a [18 U.S.C. § 3117] tracking device[,]"[199] which is what a cell phone becomes when its signals are used to determine the mobile's whereabouts. "'Real-time location monitoring effectively converts a cell phone into a tracking device . . . .'"[200] Second, the SCA relates to "stored" or historical information and not to prospectively obtained data. In other words, the statute "pertains to the production of existing records, not information that will be created in the future related to future communications."[201] Third, although the SCA provides, by exceptions, for the release of certain data to a "governmental entity,"[202] none of the exceptions reference the Pen/Trap Statute.[203] "Fourth, the pairing of the Pen/Trap statute and the SCA—which were enacted at different times (as was CALEA)—is not mentioned in any statute or

---

194 *Id.* at *4 (emphasis added).
195 *Id.* at *5 n.6.
196 *Id.* at *5 (citing SDTX#1, 396 F. Supp. 2d 747 (S.D. Tex. 2005)).
197 18 U.S.C. § 2510(15) (2000).
198 *Id.* § 2510(1), (18).
199 *Id.* § 2510(c).
200 *EDWIS#2*, 2006 WL 2871743, at *5.
201 *Id.* at *6.
202 18 U.S.C. § 2701(c).
203 *EDWIS#2,* 2006 WL 2871743, at *6 (quoting SDTX#3, 441 F. Supp. 2d 816, 834 (S.D. Tex. 2006)).

specifically discussed in the legislative history."[204] Joining most courts which have considered the issue to date, U.S. District Judge Adelman concluded her opinion by rejecting the government's hybrid theory and requiring the government to meet the probable cause standard to obtain cell site information.

S. Southern District of New York – October 2006 (SDNY#3)

In this appeal of *SDNY#2*,[205] U.S. District Judge Kaplan, apparently a strict constructionist, came to a result opposite that of Judge Adelman, finding that even though Congress may not have explicitly intended that the Pen Register Statute and the SCA be coupled together, the language of the two Acts "clearly" authorized disclosure of cell site information.[206] In constructing this conclusion, the court determined that the signals a cell phone transmits to one or more towers to make a call constitutes "signaling information" for purposes of the Pen Register Statute.[207] Turning next to the "solely pursuant" language at 47 U.S.C.

---

[204] *Id.* The Pen/Trap provisions, 18 U.S.C. §§ 3121-3127, were originally enacted as part of ECPA on October 21, 1986, amended by CALEA on October 25, 1994, and further amended by the USA PATRIOT Act on October 26, 2001. Recall that the SCA was enacted as title II of ECPA, *see supra* note 15.

[205] Only limited tracking information was sought.

[206] SDNY#3, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006). In a nod toward sanity, the court allowed that "Congress nevertheless may wish to consider whether this result is consistent with its intention." *Id.* The government here sought limited cell site location information in the hope, one would think, that its limited request would be more likely to win judicial favor. As noted earlier, however, such an approach is like arguing that one is but a little bit pregnant. The court recognized this sophistry:

> Many of the initial applications for cell site information sought information that could be used for triangulation. After these applications were rejected by many courts, however, the government began to request information regarding only one tower at a time, apparently in the hope that applications for less detailed and invasive information would meet with a warmer judicial reception. This application is part of the latter group . . . . The government's arguments for statutory authorization, however, apply equally whether information is obtained from one antenna tower at a time or from many simultaneously. *Id.* at 452 (internal citations omitted).

[207] *Id.* at 455. Before citing *United States Telecommunications Ass'n v. FCC*, 227 F.3d 450, 455 (D.C. Cir. 2000), as additional authority in support of this outcome, Judge Kaplan observed that "[a] number of the judges to address this issue have reached the same conclusion, even several who ultimately denied applications for cell site information for other reasons." *SDNY#3,* 460 F. Supp. 2d at 455. Responding unasked to those USMJs deciding to the contrary, ". . . the Court presumes that Congress knew—when it added the term 'signaling information' to the definitions of pen registers and trap and trace devices in 2001—that the D.C. Circuit had interpreted that term to include cell site information in the *United States Telecomm. Ass'n* decision a year earlier." *Id.* at 456 (citation omitted).

§ 1002(a)(2),[208] the court determined that the "most natural" reading of the provision is that cell site location information can properly be disclosed "pursuant to the Pen Register Statute *and* some other statutory authority."[209] Reaching a contrary conclusion, even if such is arguably supported by legislative history,[210] would mandate "reading the word 'solely' out of the statute entirely, which would violate 'the settled rule that the Court must, if possible, construe a statute to give every word some operative effect.'"[211] The next hurdle to the government's hybrid approach was the contention that prospective cell site information is not cognizable under the SCA. Indeed, most of decisions already discussed accepted the contention that "although [18 U.S.C. § 2703] might cover historical cell site data, [it] does not authorize the disclosure of such data on a 'real-time' or forward-looking basis."[212]

Further blocking the adoption of the hybrid approach is the argument that none of the traditional safeguards currently part of ELSUR statutes exist after pairing the SCA with the Pen/Trap Statute, e.g., there is no "limit [on] the duration of law enforcement surveillance pursuant to a court order [nor is there a] require[ment for] automatic sealing of such orders to maintain secrecy surrounding ongoing surveillance."[213] The court found this dodge "unpersuasive" because, (1) not only does the SCA not contain any surveillance time constraints which would circumscribe the collection of prospective cell site location information, but even more importantly, (2) "the information the government requests is, in fact, a stored, historical record because it will be received by the cell phone service provider and stored, if only momentarily, before being forwarded to law enforcement officials."[214] A

---

208 *See supra* note 35 and accompanying text.

209 *SDNY#3,* 460 F. Supp. 2d at 457.

210 *Id.* "Indeed, both the Senate and House Reports on CALEA asserted that the respective bills 'expressly provide[ ] that the authorization under the pen register and trap and trace orders cannot be used to obtain tracking or location information, other than that which can be determined from the phone number.'" *Id.* at 457-58 (internal citations omitted).

211 *Id.* at 458 (citation omitted).

212 *Id.* at 459.

213 *Id.* "Several of the magistrate judges and *amicus* [Federal Defenders of New York] here contend that if Congress had intended the Stored Communications Act to permit prospective surveillance, 'it would have included the same prospective features it built into the wiretap and pen/trap statutes.'" *Id.* (internal citations omitted).

214 *Id.* (citing SDNY#1, 405 F. Supp. 2d 435, 446-47 (S.D.N.Y. 2005)). The fact that there may be momentary storage should be beside the point. What should matter is that the government's application seeks information not yet in existence at the time an order would be signed. Further, *see supra* note 29, cell site location information can be pushed both to law enforcement and the service provider at the same time.

third reason supporting rejection of the amicus's argument is that the Pen/Trap Statute—to which the SCA would be metaphorically glued—does have ELSUR duration limitations which would result from a pairing with the Pen/Trap Statute.[215] A final argument raised against the marriage of the Pen/Trap Statute with the SCA is that part of the latter, 18 U.S.C. § 2711, incorporates definitions from Title III and, more particularly, the definition of "electronic communication" which, in turn, specifically excludes "any communication from a tracking device (as defined in section 3117)[.]"[216] The court also found this contention to be "unpersuasive" and even considers resolution of the question whether a cell phone meets the statutory definition of a "tracking device" to be "immaterial" because 18 U.S.C. § 2703 allows a court "upon a proper showing, to order disclosure of "a record or other information pertaining to a subscriber to or a customer of an *electronic communications service.*" It does not authorize the disclosure of an "*electronic communication.*"[217]

Cherry picking statutory provisions even further, the court also concluded that,

> because a cell phone provider is an "electronic communications service" and cell site information is a "record or other information pertaining to a subscriber to or a customer of" the cell phone provider, the logical conclusion is that Sections 2703(c) and (d) permit a court to order the disclosure of prospective cell site information upon a proper showing by the government. The Stored Communications Act, then, provides the additional authority for cell site information required by CALEA.[218]

---

[215] "The Stored Communications Act is being asked to play only the supporting role of providing the required additional authorization for the disclosure of information already permitted by the Pen Register Statute. Accordingly, it makes sense that the Pen Register Statute would provide the procedural framework." *SDNY#3*, 460 F. Supp. 2d at 459. If, as the District Judge posits, the pen/trap plays the principal role in the unclean, bizarre conjoining of the pen/trap and SCA provisions, then why does the CALEA admonition at 47 U.S.C. § 1002 against using pen/trap authority to locate cell phones not also play a primary (as opposed to supporting) role?

[216] 18 U.S.C. § 2510(12)(C) (2000). Recall that 18 U.S.C. § 3117(b) tells us that a "'tracking device' [is] an electronic or mechanical device which permits the tracking of the movement of a person or object."

[217] *SDNY#3,* 460 F. Supp. 2d at 460.

[218] *Id*. at 460-61.

The court then addressed the concern expressed by many of the earlier opinions that to the extent a cell phone is a § 3117 tracking device, an order permitting the provision of cell site location information to the government must be predicated upon probable cause. The court correctly pointed out that by its terms, 18 U.S.C. § 3117 advises that a "warrant or *other order*"[219] may be secured upon an adequate showing thus permitting court authorization to issue upon less than probable cause.[220] More significantly, the court correctly noted that § 3117 relates only to the *installation* and not the monitoring of a tracking device.[221]

Amici raised an interesting but flawed argument when they stated that, statutes aside, the Fourth Amendment mandates a probable cause-grounded warrant because *Karo*[222] requires such an order "if the device would disclose its location inside a person's home and that information could not have been observed from public spaces."[223] The court conceded that a *Karo* violation is within the universe of possibilities but that a *Karo* analysis at this juncture would be premature.[224] As a result, the court granted the government's hybrid theory-based application for limited cell-site location information.[225]

T. Eastern District of California – February 2007 (EDCA#2)

In another of the relatively few opinions favorable to the government, the same USMJ who authored *EDCA#1* recited that in an earlier order he had determined that cell site location information constituted "subscriber information accessible to law enforcement upon

---

[219] *Id.* at 461.

[220] "Accordingly, Section 3117 specifically 'contemplates that a tracking device may be installed pursuant to an 'order'—that is, without a warrant and thus without a probable cause showing'" *Id.* (internal citations omitted).

[221] *Id.* at 453; *see also* 18 U.S.C. § 3117(a).

[222] *See* United States v. Karo, 468 U.S. 705 (1984).

[223] *SDNY#3,* 460 F. Supp. 2d at 462.

[224] "At this point, however, the Court has no way of knowing if the government will use any cell site information it obtains in this manner. If it does, and information leads to indictment, the issue can be litigated on a motion to suppress." *Id.*

[225] Rather unartfully, the court stated that use of

> The pen register and/or trap and trace device is authorized to capture (1) the calls made and received by the subject cell phone and (2) information which identifies the antenna tower receiving transmissions from that cell phone at the beginning and end of a particular telephone call made or received by the telephone's user, including any information on what portion of that tower is receiving a transmission at the beginning and end of a particular telephone call.

Id. at 463. The court's phrasing is unartful because "capturing calls made and received" would require a Title III.

order"[226] grounded upon the government's hybrid theory. Note that in the course of his decision, USMJ Hollows determined that 18 U.S.C. § 3117(b) "does not include the acquisition of cell site information in the terms 'tracking device'" because that statute has to be understood in the context of when it was enacted as part of ECPA in 1986 and upon so doing, it is clear that the "device contemplated" by § 3117(b) "was only of the 'beeper' variety."[227] Looking to § 3117(b)'s legislative history, the USMJ also concluded that the acceptance of previously recorded location information from a cell phone company was not "installation of a device."[228]

Intriguingly, and in a parenthetical footnote, the court said—seemingly at variance with *Karo*[229]—that tracking a cell phone being used inside a residence is actually,

> all done outside the home via cell towers. Unless the agents are calling the suspect's phone, the agents have no control over the suspect's use of the cell phone whatever in his location, did not cause or initiate the cell phone signal, and are not keying in on the cell phone signal *inside the home*. Mathematical triangulations made from different cell phone towers outside the home which will reveal a general area where the suspect may be found is hardly probing inside the house.[230]

This Article has demonstrated that in the great majority of opinions where the matter has arisen, courts have opined that the government's hybrid or convergence approach is legally bankrupt and that only a Fourth Amendment/Rule 41 warrant is an acceptable underpinning for an order directing cell phone carriers to provide cell phone location information to law enforcement. In the discussion which follows, however, a third, largely untried option is suggested.

---

226 EDCA#2, No. 07-SW-034 GGH, 2007 WL 397129, at *1 (E.D. Cal. Feb. 1, 2007).

227 *Id.* at *2.

228 *Id* at * 1 n.1.

229 *Supra* note 7. Recall that in *Karo*, however, the tracking was made possible by a government-installed device which was emanating signals as a result of that installation.

230 *EDCA#2*, 2007 WL 397129, at *1 n.2.

III. ANALYSIS

A. Alternative Legal Foundation

Instead of continued pursuit of a legal offensive underpinned by the Pen/Trap Statute, the SCA, CALEA, or a hybrid of some or all of the three, it may be appropriate to take a step backwards and attack from a different vector, from another direction—one not based upon a precarious statutory mélange but upon fundamental Fourth Amendment law.

Knotts[231] and *Karo*[232] teach that electronically *monitoring* the changing location of an object or a person is not a search within the meaning of the Fourth Amendment so long as the shifting situs of the thing being tracked *could* be determined by visual observation made from a spot where one is legally permitted to be, e.g., from a public highway. This result follows because such observations do not intrude upon an expectation of privacy that society is prepared to recognize as reasonable. If there is no search, there is no need for a warrant based upon probable cause. So long as the surveilled person or object is neither within a curtilage that is *not* open to public observation or within a residence, there is no reasonable expectation of privacy attached to the movements of the person or object.[233]

Both cases were decided in the 1980s, i.e., a decade before CALEA, and the second decision followed closely on the heels of the first, just a year later. It may be helpful to review the facts in both of these opinions. Often there are four events in connection with the utilization of a "traditional" tracking device each of which could implicate the Fourth Amendment: installation, repair/maintenance, monitoring, and removal. Inasmuch as Knotts never contested the legality of the device's installation, the case bearing his name only concerned monitoring.[234]

---

231 United States v. Knotts, 460 U.S. 276 (1983).

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

233 Put differently, the key questions is whether, "without a warrant, the Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of [a] house." *Id*. at 715.

234 As a practical matter, there was nothing to contest: With the consent of a chemical manufacturer, Minnesota law enforcement personnel installed a "beeper" inside a 5-gallon container of a precursor chemical, chloroform, useful in the production of controlled substances. When one of the defendants bought the chloroform, the officers were able to follow it from Minneapolis to just *outside* Knott's "secluded cabin near Shell Lake, Wis[consin]." *Knotts*, 460 U.S. at 277. "Under a barrel outside the cabin, officers located the five-gallon container of chloroform." *Id*. at 279.

Law enforcement personnel were able to track a five-gallon chloroform container with a "beeper" hidden therein as it was driven to the exterior of a lakeside cabin owned by Knotts.[235] Warrantless monitoring of the "beeper" or tracking device, Knotts contended, violated the Fourth Amendment. But the Supreme Court found otherwise:

> A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the co-defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[236]

That the chloroform came to rest on private property was of no consequence because there was no reasonable expectation of privacy with respect "to movements of [conveyances and] objects such as the drum of chloroform outside the cabin in the 'open fields.'"[237] The expectation was lessened because the tracking device revealed nothing more than what the police could have seen had they chosen to tail the driver all the way to Knotts' cabin.[238] "Visual surveillance from public places along [the driver's] route or adjoining Knotts' premises would have sufficed to reveal all of these facts to the police."[239] Since the monitoring did not invade any legitimate expectation of privacy, neither a search nor a seizure under the Fourth Amendment took place.[240]

The facts in *Karo* were surprisingly similar. Karo and his co-defendants ordered fifty gallons of ether which were to be used to extract cocaine from imported clothing previously impregnated with the

---

[235] Based upon information in addition to that supplied by the tracking device, law enforcement personnel secured a search warrant, raided the cabin, and discovered an "operable" clandestine drug laboratory containing enough precursors "to produce 14 pounds of pure amphetamine." *Id*.

[236] *Id.* at 281-82. Knotts "undoubtedly had the traditional expectation of privacy *within* a dwelling place insofar as the cabin was concerned[.]" *Id.* at 282 (emphasis added).

[237] *Id*. (citing Hester v. United States, 265 U.S. 57 (1924)).

[238] "But there is no indication that the beeper was used in any way to reveal information as to the movement of the drum *within* the cabin, or in any way that would not have been visible to the naked eye from outside the cabin . . . . [N]otions of physical trespass based on the law of real property [are] not dispositive." *Id*. (emphasis added).

[239] *Id.*

[240] *Id.*

drug, but unfortunately for Karo, the vendor he chose was an informant who permitted DEA to substitute an ether container equipped with a tracking device.[241] DEA was thus able to track the container's rather circuitous route as it was transferred from place to place and vehicle to vehicle, until it was driven to a house rented by three of Karo's co-defendants. Because of the threat of compromise, the agents were unable to conduct tight visual surveillance, and thus did not know whether the ether remained in a vehicle parked outside or had been moved in or around the house. After all of the defendants' vehicles left, however, agents could tell by the signal from the at-rest tracking device that the ether remained at the house.

The vendor's consent obviated the need for an installation warrant, but was a court order nonetheless needed to monitor the tracking device that had been hidden in the ether container? The question was squarely presented to the Supreme Court: does "monitoring of a beeper in a private residence, a location not open to visual surveillance, violate[ ] the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence[?]"[242] Concluding that the Fourth Amendment had been contravened in this instance, the court was quick to contrast the facts with those in *Knotts*, "for there the beeper told the authorities nothing about the *interior* of Knotts' cabin."[243] Here, on the other hand, "the Government surreptitiously employ[ed] an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house."[244] As a result, the court maintained

---

[241] In addition to the vendor's consent allowing installation of the tracking equipment, DEA had obtained a warrant permitting both installation and monitoring. United States v. Karo, 468 U.S. 705, 708 (1983). Defendants successfully challenged the sufficiency of the warrant (because it contained misleading statements) which left the Supreme Court to determine the legality of the (now) warrantless installation and monitoring. *Id.* at 710, 718 n.5.

[242] *Id.* at 714.

[243] *Id.* at 715 (emphasis added).

[244] *Id.*

> The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if the 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.

Id. But is this comment accurate? If circumstances were otherwise and had there been no concern about the compromise of physical surveillance, DEA could have ringed the house 360° with binocular-equipped agents and would have learned the same information reported by the tracking device—that the ether had been moved from a vehicle to the inside of the house where it then remained. The device was not, apparently, sufficiently

"the general rule that a search of a house should be conducted pursuant to a warrant."[245]

Twenty years after *Knotts* and *Karo,* the Sixth Circuit got it right. Recall the facts in *Forest*[246]—DEA dialed the cell phone of one of the defendants (but did not let the phone ring). DEA then queried the service provider and learned what cell towers were being "hit" by the phone, thus learning the defendant's general location. This enabled DEA to re-establish physical surveillance of the target. Among other things, the defendant argued that DEA "effectively turned his cellular phone into a tracking device . . . ." in violation of his Fourth Amendment rights.[247] Forest tried to argue that the facts in his case were different from those in *Knotts* and that the "cell-site data provided information that the DEA agents could not have obtained simply by following his car."[248] But it is not what the agents saw or did not see that matters; rather, it is what *could* have been observed by third parties that counts. The court emphasized that "[a]lthough the DEA agents were not able to maintain visual contact with [the defendant's] car at all times, visual observation was *possible* by any member of the public. The DEA simply used the cell-site data to 'augment[ ] the sensory faculties bestowed upon them at birth,' which is permissible under *Knotts*."[249]

The defendant then argued that if he did not have a reasonable expectation of privacy with respect to his location, he did have one with respect to the "cell-site data itself."[250] This protection existed, according to the defendant, because: (1) unlike the situation presented in *Knotts*,

---

discriminating or accurate to reveal in which room or on which floor the ether came to rest. Because the device disclosed no information in addition to what could have been discovered by 360° visual surveillance, arguably the Supreme Court was incorrect in its analysis and no monitoring warrant should have been required. The tracking device indicated only that it was inside the house and at no point did it reveal what law enforcement personnel could have discerned with the five senses had they been inside the residence in lieu of the tracking device. *Cf.* Kyllo v. United States, 533 U.S. 27 (2001) (use of thermal imaging device to detect heat emanating from the interior of a residence constitutes a search). "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." *Id.* at 34 (internal citations omitted).

245 *Knotts*, 460 U.S. at 718.

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

247 *Id.*

248 *Id.* at 951.

249 *Id.* (internal citations omitted).

250 *Id.*

neither the transmitting nor receiving instruments belonged to the government; (2) the defendant's contract with the service provider did not authorize disclosure of his cell-site data; and (3) the information DEA obtained by "pinging" his phone was not the result of any affirmative action on his part, i.e., unlike the situation in *Smith v. Maryland*,[251] because he had not dialed any outgoing digits nor was he in communication with anyone when DEA dialed his phone.[252] The Sixth Circuit was unimpressed, opining that any difference between the defendant's location and his cell-site data was one without a distinction.[253] Given the facts of the case, it simply was "not legally significant" because the "cell-site data is simply a proxy for [the defendant's] observable location."[254] Consequently, the court found *Knotts* to be controlling and thus concluded that DEA had not conducted a Fourth Amendment search.[255]

Contrary to the warning expressed in *DMD#1*, law enforcement *has* historically acted at "its peril" and yet suffered no epidemic of adverse consequences by engaging in the warrantless, electronic monitoring of tracking devices installed within or on conveyances and objects that travel on publicly accessible highways, waters, and airspace. Where is the legal consistency in requiring a different result just because the location-identifying equipment belongs to parties other than the government? The nature of the information obtained by the government is the same, whether from its own radio equipment or from a cell phone service provider.[256] The majority of USMJs, having lost sight of this, are letting the tail wag the dog.

Concededly, it is certainly possible and permissible for a statute to impose more stringent requirements upon police during the performance of law enforcement activity than constitutionally provided

---

[251] Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979).

[252] *Id.*

[253] *Id.*

[254] *Forest*, 355 F.3d at 951.

[255] *Id.* at 951-52.

[256] When government-owned devices are utilized, law enforcement has dominion and control over the receiver and has at least dominion over the transmitter. When cell phones are tracked, the transmitter, i.e., the cell phone, is controlled by the user and the receiving equipment is typically within both the dominion and control of the service provider. *Installation* of a government-owned device will often require an intrusion to install the device; such an incursion in many instances occasions the infringement of a privacy interest that society would judge to be reasonable thus necessitating a Rule 41 warrant. However, no installation need be effected when a cell phone is the tracking device. Thus, the use of a cell phone to determine a user's location can be less invasive than utilization of a government setup.

baselines. However, neither the Pen/Trap Statute nor § 2703 imposes even a probable cause requirement and, in any event, seventeen of the cases just discussed determined that the two laws are simply inapplicable.[257] As already mentioned, this is because (1) the Pen/Trap Statute cannot be applied to cell phone tracking inasmuch as 47 U.S.C. § 1002(a)(2)(B), part of CALEA, instructs that the specific location or call-identifying information such "devices" *can* provide "shall not include any information that may disclose the physical location of the subscriber"; and (2) § 2703 relates to stored or historical information as opposed to that which is acquired—as is also the case with Title III orders and pens/traps—in real-time.

B. Director Freeh's Remarks in Context

At least three of the USMJ cases[258] discussed Director Freeh's 1994 remarks, which were made immediately prior to CALEA's passage so it would do well to correctly understand the historical timeframe in which they were made.[259]

As previously noted,[260] the Pen/Trap Statute was enacted as part of ECPA in 1986, and it was then that both apparatuses were first defined: they were both declared to be "devices"[261] and *not* "devices" plus "processes"—as has been the case ever since the instruments' meanings were amended fifteen years later by the 2001 USA PATRIOT Act.[262] In short, at the time when Director Freeh presented his 1994 prepared statement to the joint meeting of the Hill subcommittees, pen registers as

---

257 *But cf.* Title III *vis-à-vis* the Fourth Amendment.

258 *See* EDWIS, 412 F. Supp. 2d 947 (E.D. Wis. 2006); WDNY, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); DDC#2, 407 F. Supp. 2d 132 (D.D.C. 2005).

259 Louis J. Freeh, Director, F.B.I., Statement before the Senate Judiciary Subcommittee on Technology and the Law and the House Judiciary Subcommittee on Civil and Constitutional Rights (Mar. 18, 1994), *reprinted in* Federal Document Clearing House, 1994 WL 223962 [hereinafter Freeh Testimony].

260 *See supra* notes 226-27 and accompanying text.

261 *See supra* note 1. The ECPA set forth the definitions of both terms at Section 103 thereof. Section 103, in turn, set forth original chapter 206 of 18 U.S.C. which included the definition of "pen register" at what was then (1986), the new 18 U.S.C. § 3126(3), as

> a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer [for billing, recording as incident to billing, cost accounting, or other like purpose].

Similarly, (then) new 18 U.S.C. § 3126(4) defined "trap and trace" as a "device which captures incoming or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted[.]"

262 These amendments occurred some seven years after Director Freeh's testimony.

well as trap and trace devices were somewhat rudimentary mechanical instruments that required physical connection to telephone wires in order to be able to print out the digits customers actually dialed, as well as the times of day traditional telephones went on and off-hook when making or receiving calls. The pen/trap devices, as statutorily defined in 1986, were thus incapable of determining cell phone locations—a not unusual instance where legislation lagged behind technological advance. According to a cell phone industry association, the use of cell phones in the United States did not even *commence* until the mid-1980s. [263]

Examined against this backdrop, at the time Director Freeh's remarks were presented to the two subcommittees meeting jointly, pen/trap "processes" made possible by computer software which would permit the record-keeping of some cell phone location information was a somewhat distant, if not unimagined vision—especially for law enforcement investigative uses—which explains his somewhat indefinite comment that "[s]ome cellular carriers do acquire information relating to the general location of a cellular telephone for *call distribution* [as opposed to user tracking] *analysis purposes*."[264] Thus, the entire portion (captioned *Allegations of "Tracking" Persons*[265]) of his prepared statement must be viewed through this lens. The practice of securing real-time cell phone location information for law enforcement purposes from wireless service providers was in its infancy, and could not yet be considered an arrow in the police quiver. Thus, Director Freeh conceived of cell phone location information as data only for business—"call distribution analysis purposes"—and not, in his words, for the sort of "true tracking" engaged in by law enforcement for criminal investigative purposes.

Yet "true tracking" was the practice discussed in both the *Knotts* and *Karo* decisions, of which the Director was well aware.[266] Both matters

---

[263] According to the Cellular Telecommunications and Internet Association—The Wireless Association, the first commercial cellular system began operation in the United States (Chicago) in October 1983; the second system started in December 1983 in the Baltimore/Washington, D.C. corridor. By 1986, there were only 1,000 cell sites in the country. There were 10 million cell phone users in the U.S. by 1992 and 10,000 cell sites. By 1997, the number of cell sites had risen to 50,000. There are now over 100 million wireless subscribers in the U.S. *See generally* Cellular Telecommunications and Internet Association—The Wireless Association, The History of Wireless, http://www.ctia.org/content/index.cfm/AID/101 (last visited Apr. 7, 2007).

[264] *See* WDNY, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) (emphasis added); Freeh Testimony, *supra* note 259 (emphasis and explanation provided).

[265] *See* Freeh Testimony, *supra* note 259, at 32-33.

[266] Director Freeh even provided a citation to *United States v. Karo*, 468 U.S. 705 (1984), *supra* note 259.

were decided a decade before the Director's statement and held that no Fourth Amendment probable cause orders/warrants were needed to track the movements of suspects traveling out in public. Conversely, "'true' tracking" "require[s] a warrant or court order when used to track *within a private location not open to public view.*"[267] Cell phone location "transactional" information obtained and retained for business purposes--and thus not "true tracking" information—could be secured from the service providers by law enforcement with either "*court orders* or *subpoenas*" as set forth in 18 U.S.C. § 2703.[268] The Director knew the difference between subpoenas, court orders, and warrants. Warrants were needed for real-time tracking *if* the target were "within a private location not open to public view." No warrants were required, therefore (as *Knotts* and *Karo* instructed), for all other real-time tracking.

Thus, when Director Freeh said that "call setup information"—real time dialing data traditionally obtained by pen/trap instruments which "identifies the origin and destination of a wire or electronic communication,"[269]—would not also "include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange,"[270] he was speaking of the information then known to be obtainable by pen/trap instruments. This "call setup information" was in contrast with "transactional" data, which includes generalized location information that in 1994 was understood to be data kept by carriers "for call distribution analysis purposes" and thus considered to be historical records that law enforcement could obtain "exclusively" via 18 U.S.C., chapter 121 (the SCA).[271]

Put differently, and in Director Freeh's mind, the CALEA caveat codified at 47 U.S.C. § 1002(a)(2)(B)—which provides that call-identifying information obtained by pens/traps "shall not include any information that may disclose the physical location" of the subscriber—had nothing to do with and cannot be seen as a restriction upon real-time cell phone location information that carriers are today (well post-1994)

---

267 *Karo*, 468 U.S. 705.

268 *See* Freeh Testimony, *supra* note 259, at 33 (emphasis added) (recalling that ECPA, including 18 U.S.C. §§ 2701-2710, the SCA, was enacted in 1986—eight years before the Director's testimony).

269 E-mail is an example of an "electronic communication" and, in that context, an example of a "communication address" that is "similar" to a telephone number would be an e-mail address.

270 *Id.*

271 *Id.* at 31.

capable of providing via pen/cell "processes" to law enforcement. In order to engage in a legislative history analysis, the 1994 CALEA constraint upon pen/trap "devices" cannot be applied to 2006 pen/trap "processes."

C. Operating in "Peril"

Recall that the *DMD#1* USMJ cautioned that "[t]o 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."[272] This remark is consistent with the aforementioned 1994 testimony of FBI Director Freeh as well as the lessons from both *Knotts* and *Karo*. The majority of the USMJs failed to latch on to the seemingly obvious notion that the cell phone location data sought by the government from the service providers did not—according to the facts of each case—originate from such a private place. Thus, no probable cause-based court orders or Rule 41 search warrants were constitutionally required to conduct the location surveillance requested.

Further, the exactitude of real time cell phone location information currently available from service providers is insufficient to determine the floor or room within a residence where the cell phone user is situated. Thus, if all that current, technologically obtainable real time cell phone location data can reveal is that a suspect is inside a residence, how can this information nugget be more invasive than the visual observation to the same effect by agents armed with binoculars encircling the area?[273]

---

[272] *See supra* note 1 and accompanying text (emphasis added).

[273] *See* United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (recalling that "cell-site data is simply a proxy for [the cell phone user's] observable location"). Let's assume for the sake of argument—binoculars aside for the moment—that a police determination of the target's *mere presence* (without more) inside a residence or protected-from-view curtilage is an invasion of privacy that society would recognize to be unreasonable absent a warrant. Should the chance, even if remote, that the suspect may venture into a residence (his? hers? someone else's?) preclude a law enforcement agency from securing cell phone location information from a wireless service provider? Even if this were the case, a suggested work-around would be to borrow from the minimization requirements of Title III [18 U.S.C. § 2518(5)] so that at such time as it became apparent that the subject was about to enter a constitutionally-protected area, the law enforcement agency would cease reception of the cell phone location information from the service provider subject, of course, to the periodic re-initiation of reception every several minutes to ensure that the target has not departed. Note that in the case of foreign language Title III (communication content) intercepts, even *after-the-fact* minimization is permissible in certain instances, 18 U.S.C. § 2518(5): "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception."

The *DMD#1* USMJ was more on the mark than perhaps he realized when he said that, "[i]f 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."[274]

Bingo. How is it, then, that the USMJs proceeded from the unremarkable but prescient statement just quoted to the mandate that such information can be procured only with a Rule 41 warrant? It truly boggles the mind; certainly logic does not inspire (let alone compel) such a conclusion.

D. Federal Rule of Criminal Procedure 57, the All Writs Act, and the Inherent Power of the Courts

As indicated earlier, before the Pen/Trap Statute was enacted in 1986, the situation was not unlike it is today with cell phone location information: an order compelling the assistance of a third party was needed so that law enforcement could gain access to information it needed to further a criminal investigation—even though the order was not constitutionally mandated inasmuch as the desired information was unworthy of constitutional protection. [275] The absence of a statute specifically setting forth a regime for pen/trap orders did not meaningfully hinder law enforcement prior to 1986. Effective orders were secured using a combination of Federal Rule of Criminal Procedure 57(b) ("Rule 57"),[276] the All Writs Act,[277] and the court's inherent power. Use of these in combination, although suggested by dicta in *United States*

Certainly the interception of communication content impinges upon Fourth Amendment considerations much more than does cell phone user location information.

274 *See* DMD#1, 402 F. Supp. 2d 597, 604 (D. Md. 2005).

275 *See supra* note 28 and accompanying text.

276 Rule 57(b) reads in part that "[a] judge may regulate practice in any manner consistent with federal law, these rules, and local rules of the district." *See also* SDTX#3, 396 F. Supp. 2d 747, 830 n.31 (S.D. Tex. 2005).

277 All Writs Act, 28 U.S.C. § 1651 (2000), states

> (a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law. (b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

A rule or *decree nisi* is "[a] court's decree that will become absolute unless the adversely affected party shows the court, within a specified time, why it should be set aside." BLACK'S LAW DICTIONARY 441 (8th ed. 2004).

v. New York Telephone Co.[278] proved to be a workable, pre-Chapter 206 stratagem.[279]

Instead of using the largely unsuccessful hybrid theory, federal prosecutors should consider steering clear of the inapplicable Section 2703, the Pen/Trap Statute, and CALEA (that well is already poisoned) and instead rely upon the arguments found successful in *Knotts*,[280] *Karo*,[281] and *Forest*[282] when seeking an order based upon Rule 57(b), the All Writs Act, and the court's inherent authority. Although the Justice Department frowns on such an approach, it certainly could not fare any worse than proceeding upon the hybrid theory.

Of the USMJ decisions chronicled above, only three discussed the Rule 57(b) and/or the All Writs Act approach, *EDNY#2*, *SDTX#3*,[283] and, in passing, *WDNY*.[284] Although the *EDNY#2* USMJ did not question the "correctness" of the earlier decisions upholding orders based upon the All Writs Act, he nevertheless "conclud[ed] that they [did] not advance the government's cause here."[285] This was because the decisions

---

[278] United States v. N.Y. Tel. Co., 434 U.S. 159, 170 (1977). At the time *New York Telephone Co.* was decided, Rule 57(b) read that "[i]f no procedure is specifically prescribed by rule, the court may proceed in any lawful manner not inconsistent with these rules or any applicable statute." *Id.* The communication carrier in *New York Telephone Co.* had refused to help the FBI install a pen register despite the existence of an order supported by probable cause, arguing that an order adhering to the more stringent Title III standard was required. *Id.* Although we now know from a subsequently decided case that probable cause need not have been proffered, *see* Smith v. Maryland, 442 U.S. 735 (1979), the FBI had, in fact, grounded its application upon that level of proof. Even though Rule 41, by its terms, spoke only of solid objects until this past December, the rule was "not limited to tangible items but [was] sufficiently flexible to include within its scope electronic intrusions . . . ." *N.Y. Tel. Co.*, 434 U.S. at 169. Buttressing that conclusion, the court remarked that its

> conclusion that Rule 41 authorizes the use of pen registers . . . is supported by Fed. Rule Crim. Proc. 57 (b). . . . Although we need not and do not decide whether Rule 57(b) by itself would authorize the issuance of pen register orders, it reinforces our conclusion that Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers as well as tangible items.

Id. at 170.

[279] *See, e.g.*, United States v. Mosko, 654 F. Supp. 402, 405 (D. Colo. 1987) (pre-ECPA/All Writs Act order issued for pen register operations).

[280] United States v. Knotts, 60 U.S. 276 (1982).

[281] United States v. Karo, 468 U.S. 705 (1984).

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

[283] SDTX#3, 441 F. Supp. 2d 816, 831 n.31 (S.D. Tex. 2006).

[284] In a footnote, the *WDNY* USMJ simply adopted the position advanced by the *EDNY#2* USMJ. WDNY, 415 F. Supp. 2d 211, 219-20 n.7 (W.D.N.Y. 2006).

[285] EDNY#2, 396 F. Supp. 2d 294, 325 (E.D.N.Y. 2005).

championed by the government were, in the USMJ's view, not sufficiently on all fours with the facts before him. In *United States v. Mosko*, for example, the defendant challenged the pen register evidence against him on the ground that the underlying order should have been based upon probable cause.[286] In rejecting the defendant's suppression request, the *Mosko* court correctly cited to *Smith*[287] when observing that a pen register order need not be grounded upon probable cause and—without embellishment or conclusion—observed that the pen register order had been secured in reliance upon the All Writs Act. "Second," remarked the court in *EDNY#2*, "none of the cited cases relied on the All Writs Act to trump existing statutory law governing the use of investigative techniques, nor did any of them purport to fill a gap in an existing statutory scheme."[288] In should be pointed out, however, that the *Mosko* court was aware that the Pen/Trap Statute had been passed but determined that the provision had no retroactive effect such that it would impact upon the facts of the case at bar. Thus, the court was aware that the All Writs Act approach *did* fill a *legislative* weakness not repaired until the enactment of ECPA.[289]

Although the *Mosko* court did not expressly rule on the propriety of securing a pre-ECPA pen register authorization with an All Writs Act order, this does not obliterate the fact that such an All Writs Act order allowing pen register operations was sustained. It is certainly plausible to suggest that the *Mosko* court did not directly address the All Writs Act issue because: (1) law enforcement use of a pen register simply does not implicate any privacy interests secured by the Constitution and thus there was no longer a basis left upon which the defendant could successfully fashion a suppression argument; and because (2) the defendant never contended that the All Writs Act was an insufficient foundation upon which to underpin a pen register order.

The *EDNY#2* USMJ saw the chasm but either could or would not make the leap:

> The government thus asks me to read into the All Writs Act an empowerment of the judiciary to grant the executive branch authority to use investigative techniques either explicitly denied it by the legislative branch, or at a minimum omitted from a far-reaching

---

286 United States v. Mosko, 654 F. Supp. 402, 405 (D. Colo. 1987).
287 Smith v. Maryland, 442 U.S. 735 (1979).
288 *EDNY#2*, 396 F. Supp. 2d at 326.
289 *Mosko*, 654 F. Supp. at 405 n.1.

> and detailed statutory scheme that has received the legislature's intensive and repeated consideration. Such a broad reading of the statute invites an exercise of judicial activism that is breathtaking in its scope and fundamentally inconsistent with my understanding of the extent of my authority.[290]

The fact of the matter, as actually demonstrated by *Mosko*, is that when Congress either fails to act *or has not yet acted* (as in the case where investigative practice or technological advancements outpace existing statutory provisions), or simply has not thought to act, legal workarounds are fashioned, and many succeed—again, as in *Mosko*—until the law catches up. Certainly "sneak and peek" searches were conducted before 18 U.S.C. § 3103a was enacted as part of the USA PATRIOT Act.[291] From the *ELSUR* arena, recall that when Title III intercept targets speak in code or use a language for which law enforcement does not have a translator immediately available, after-the-fact minimization is statutorily permitted.[292] Before 18 U.S.C. § 2518(5) was amended to legislatively permit such an operational approach, however, such after-the-fact minimization had been judicially sanctioned before Congress could change the law to effect a "catch up" with existing practice.[293] This is the same scenario faced now with respect to cell phone tracking—no statute specifically addresses the topic, and a work-around, such as with Rule 57(b) and the All Writs Act, should be fashioned until such time as Congress may act on the matter, especially since the DOJ's hybrid theory has been so underwhelming.

E. Voluntarily Conveying Information to Third Parties

In the course of reaching its conclusion that "[t]he installation and use of a pen register . . . was not a 'search,' and no warrant was required [to conduct pen register operations,]"[294] the Supreme Court in *Smith v.*

---

290 *EDNY#2*, 396 F. Supp. 2d at 326.

291 USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); *see*, *e.g.*, United States v. Pangburn, 983 F.2d 449 (2d Cir. 1993). "A sneak and peek warrant is one that authorizes officers to secretly enter (either physically or electronically), conduct a search, observe, take measurements, conduct examinations, smell, take pictures, copy documents, download or transmit computer files, and the like; and depart without taking any tangible evidence or leaving notice of their presence." Charles Doyle, *Terrorism: Section by Section Analysis of the USA PATRIOT Act*, CONG. RES. SERV. at 9 (Dec. 10, 2001), *available at* http://www.epic.org/privacy/ terrorism/usapatriot/RL31200.pdf.

292 *See supra* note 73.

293 *See*, *e.g.*, United States v. London, 66 F.3d 1227, 1236-37 (1st Cir. 1995); United States v. Cale, 508 F. Supp. 1038, 1041 (S.D.N.Y. 1981).

294 Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

Maryland[295] analogized the circumstances surrounding one who dials digits from a phone (and thus conveys those numbers to a third party, i.e., the telephone company) to that of a customer providing personal financial information to a bank with whom the customer conducts business.[296]

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[297]

Thus, one who carries a cell phone about—depending upon one's perspective—is doubly cursed: not only does the user lack any reasonable expectation of privacy with regard to his/her movements out in public, s/he is also damned with respect to the numbers s/he dials because those digits are voluntarily conveyed to the service provider. The user "assumes the risk" that any information s/he surrenders to a third party will be provided to law enforcement authorities. Despite arguments from some of the USMJs to the contrary,[298] this same argument holds true with regard to the cell phone location information a user broadcasts every time the instrument is turned on. Just as no one

---

[295] *Id.*

[296] This analogy was based on the facts in *United States v. Miller*, 425 U.S. 435 (1976). Congress was so unhappy with the *Miller* decision, which was constitutionally based, that it passed a law to statutorily protect the financial information customers pass along to their banking institutions. *See* the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (2000).

[297] *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 443).

[298] Discussing both *Smith* and its treatment by *Forest*, the *SDTX#1* USMJ said "[u]nlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge." SDTX#1, 396 F. Supp. 2d 747, 756-57 (S.D. Tex. 2005). According to the *SDTX#1* USMJ, *Forest* concluded that *Smith* was inapplicable to cell phone location information. *Id.* at 757. Even if *Forest* could be read to that effect, this is flawed reasoning. The registration may be "automatic" but it is the user who sets everything in motion—thus causing the registration—by voluntarily turning the cell phone on or, if it is on, by consciously electing not to turn it off. The user thus has "control" over the registration process. A telephone user presses a speed dial button and the instrument automatically phones a number; a telephone user presses a power button and the instrument automatically registers.

forces a bank customer to do business with a financial institution, no one forces a target to use a cell phone. It is the user's conscious decision to activate and operate the instrument and s/he "assumes the risk" that the service provider will turn over to law enforcement the location information that the user broadcasts while carrying about a cell phone in operation.

F. 18 U.S.C. § 3117

There are only two places in Title 18 where the term "tracking device" is used: once within Title III at 18 U.S.C. § 2510(12)(C),[299] and again within § 3117 itself. Perhaps meaningfully, the term is nowhere to be found in either the Pen/Trap Statute, CALEA, or the SCA. The ECPA, the same public law which brought forth both the Pen/Trap Statute and the SCA, was the same act which also added Section 3117 to Title 18.[300] "Tracking device," therefore, was certainly a term of which Congress was well cognizant. If either the Pen/Trap Statute or the SCA were meant to govern tracking operations, surely Congress knew to say so, particularly in the same bill, but it did not, which strongly suggests that neither the Pen/Trap Statute nor the SCA was intended or meant to govern electronic tracking. It is certainly a canon of statutory interpretation that a law whose language is drafted generally will be trumped by one written more specifically or precisely.[301]

It is also black letter law that legislative history is not consulted if the statute to which it relates is clear on its face.[302] The problem with this particular adage, of course, lies in its application (the devil is always in the details): a law that is clear to one person is cloudy to the next. That said, if one begins with the words of 18 U.S.C. § 3117, we know that it

---

[299] 18 U.S.C. § 2510(12)(C), which references 18 U.S.C. § 3117, provides that the term "electronic communication" does not include "any communication from a tracking device (as defined in section 3117 of this title)[.]" In other words, no part of Title III covers tracking device operations.

[300] ECPA, Pub. L. No. 99-508, § 108, 100 Stat. 1848 (1986), codified as 18 U.S.C. § 3117. Recall that Title III was passed in 1968, the ECPA was enacted in 1986, and CALEA became law in 1994.

[301] Where one statute deals with a subject in general terms, and another deals with a part of the same subject in a more detailed way, the two should be harmonized if possible; but if there is any conflict, the latter will prevail, regardless of whether it was passed prior to the general statute, unless it appears that the legislature intended to make the general act controlling.

2B NORMAN J. SINGER, STATUTES AND STATUTORY CONSTRUCTION § 51:05, at 244-46, 248, 256-57 (6th ed. 2000).

[302] *Id.* at vol. 2A, § 46:01, pp. 118-19.

defines "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[303] A cell phone easily falls into this category. By its terms, the statute also tells us that court permission to use a "tracking device" can come by way of "a warrant or *other* order."[304] (Unfortunately, the provision fails to instruct which "other order" would be satisfactory.) What the statute does not say is telling—there is no requirement that the "other order" be based upon probable cause. Thus, we might properly conclude that court authorization need not be in the form of a warrant and resultantly need not be based upon probable cause. 18 U.S.C. § 3117(a) does not even make it clear whether court authorization is required in all instances before electronic/mechanical tracking device operations can commence; it merely recites that "[i]f a court is empowered to issue a warrant or other order for the *installation* of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction."[305] This begs the question whether a court order to "use" a tracking device is required if the "device" does not require installation.

If we dare turn to § 3117's legislative history, the waters get somewhat muddied. The relevant Senate Report says that "electronic tracking devices (transponders) . . . are one way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment,[306] and allows the user[307] to trace the geographical location of the transponder [with] [s]uch 'homing' devices[.]"[308] If a "tracking device" is a one-way radio, how can such an instrument be a cell phone? The section-by-section analysis of the bill which became ECPA does not shed much additional light on an understanding of the provision. It reaffirms that a "tracking device" is "an electronic or mechanical device which permits the tracking of movement of a person or object."[309] It also restates that § 3117 "provides that if a court is empowered to issue a warrant or other order for the

---

303 18 U.S.C. § 3117(b). Note, too, that the § 3117 definition of "tracking device" applies only within that section. *Id.* In other words, a "tracking device" as defined for § 3117 purposes does not necessarily hold the same meaning elsewhere.

304 *Id.* § 3117(a) (emphasis added).

305 *Id.* (emphasis added).

306 Does a cell tower qualify as "special tracking equipment?" One would not think so.

307 In this statutory instance, the "user" is the one with the radio receiver, not the "transmitter." A cell phone, of course, transmits and receives. Cell phone owners, subscribers, customers, etc., are generally considered "users" and not third parties attempting to determine the users' whereabouts.

308 S. REP. NO. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564.

309 *Id.*, *reprinted in* 1986 U.S.C.C.A.N. at 3588.

installation of a mobile tracking device" it may do so regardless of what Federal judicial districts the tracked person or object traverses—"even outside the jurisdiction of the United States[.]"[310] The report adds that "[t]his [jurisdictional] clarification does not effect [*sic*] current legal standards for the issuance of such an order."[311] Recall, then, that ECPA and § 3117 were enacted in 1986 post-*Knotts* and post-*Karo* (which, as discussed earlier, held that no court authorization was required to electronically track one's journeys on public thoroughfares), but before the 1994 passage of CALEA.

In short, looking only at § 3117 strongly suggests that a cell phone is or qualifies as a tracking device within the meaning of that section. Looking at the legislative history, however, leaves one with the impression that Congress had little clue about what technology was coming down the pike. As previously discussed, cell phones did not start being widely marketed in the U.S. until the mid-1980s so this is not necessarily surprising. Thus, it would appear that at least in this instance, the statutory language Congress came up with was drafted in such a manner as to preclude being artificially locked in by the state of technology as it existed in 1986, i.e., in the face of this chronology the statute's legislative history should not be viewed as determinative. It would appear clear that on the statute's face, a cell phone easily fits within the term "tracking device" and that this language is more direct and particularized than the more generalized language found in the Pen/Trap Statute and in the SCA, the latter two provisions being laws which others contend relate also to tracking devices or processes.

G. CALEA Does Not Preclude Application of the All Writs Act and Rule 57(b)

At its heart, 47 U.S.C. § 1002 is a "capability requirements" provision setting a minimum standard or floor that telecommunications carriers had to meet in order to, among other things, ensure that law enforcement would continue to have lawful access to wire and electronic communications in the face of fast-paced technological innovation and advancement in telecommunications. It did not preclude the industry from designing its architecture—for its own purposes—to do more than the CALEA "floor." Indeed, 47 U.S.C. § 1002(b)(1) specifically precluded law enforcement from requiring the adoption by industry or prohibiting the industry's implementation of any particular technology.[312] In other

---

310 *Id.*, *reprinted in* 1986 U.S.C.C.A.N. at 3587-3588.

311 *Id.*, *reprinted in* 1986 U.S.C.C.A.N. at 3588.

312 47 U.S.C. § 1002(b)(1) (2000) states that,

words, the government could tell the industry what minimum capabilities were required but could not tell it how to achieve those minimums. Thus, when 47 U.S.C. § 1002(a)(2) mandates that providers must have the capability of "expeditiously isolating and enabling the government, pursuant to a *court order or other lawful authorization*, to access call-identifying information that is reasonably available to the carrier,"[313] it did not require the government to secure a court order in all instances and it did not, in those instances where a court order might be necessary or desirable, direct that the order be a warrant, i.e., grounded upon probable cause. If the government, however, wanted access to call-identifying information for law enforcement purposes[314]—to the extent it would not be revealed in a very general sense by the user's area code[315]—it must underpin its application for an order (indeed, if an order were needed[316]) with a legal basis either in addition to or other than the Pen/Trap Statute.

H. Does the SCA Fit in Anywhere?

Because neither the SCA nor the Pen/Trap Statute specifically relates to "tracking devices," "work-arounds" using the pair either singly or as a statutory duo is like trying to fit a square peg into a round hole.[317] As a number of the USMJs point out, the SCA does not contemplate yet-to-be-acquired information: it is not, temporally speaking, a forward-looking

---

> [t]his subchapter [47 U.S.C. §§ 1001-1010] does not authorize any law enforcement agency or officer—(A) to require any specific design of equipment, facilities, services, features, or system configurations to be adopted by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services; or (B) to prohibit the adoption of any equipment, facility, service, or feature by any provider of a wire or electronic communication service, any manufacturer of telecommunications equipment, or any provider of telecommunications support services.

313 *Id.* § 1002(a)(2) (emphasis added).

314 As opposed to concerns relating to emergency fire and medical service. *See, e.g.*, 47 C.F.R. § 20.18 (2006).

315 Now that telephone numbers are "portable," there is no longer any assurance that the user's area code will even remotely reveal the general geographic area where the user makes or receives calls. For example, someone in Virginia can have and use a Maine area code. *See, e.g.*, 47 C.F.R. § 52.20-52.33 (2006).

316 An order might be necessary if third party assistance, although needed, was not voluntarily forthcoming.

317 Congress really needs to step in. "The use of real time cell site information by law enforcement for tracking purposes is a relatively new law enforcement tool and Congress has yet to provide specific legislative boundaries on the practice." SDIND, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *6 (S.D. Ind. June 30, 2006).

statute. It relates to wire or electronic communication *contents* in *storage*[318] and to "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication or remote computing service provider] (not including the contents of the communications)[.]"[319] In order to obtain anything more than rudimentary information,[320] the government must use either a warrant[321] or a court order,[322] the latter being authorized upon a government offering of "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."[323]

The statutory definitions applicable to the SCA do not reflect a meaning for "records or other information." [324] "Record" would suggest "already existing" data[325] which, if one had probable cause, could also be secured with a Rule 41 search warrant. But to what does "other information" potentially refer? Its meaning is certainly not self-apparent and could conceivably mean anything other than communication contents. The legislative history illustrates the term with non-exclusive examples, "customer lists and payments,"[326] which—one could logically argue—are not in the same category as cell phone location data.

I. How Does the Pen/Trap Statute Come into Play?

We know how the Pen/Trap Statute was worded when it was first enacted[327] but do we know why its wording was altered from the definition as originally signed into law? By using text italics and strikeouts, we can observe how in 2001 the USA PATRIOT Act amended the term "pen register" to now be

---

318 18 U.S.C. § 2703(a)-(b) (2000).
319 *Id.* § 2703(c).
320 *Id.* § 2703(c)(2).
321 *Id.* § 2703(c)(1)(A).
322 *Id.* § 2703(c)(1)(B).
323 *Id.* § 2703(d).
324 *Id.*
325 As opposed to future-occurring location information.
326 18 U.S.C. § 2703(c)

> permits the provider of the service to divulge, in the normal course of business, such information as customer lists and payments to anyone except a government agency. It should be noted that the information involved is information about the customer's use of the service not the content of the customer's communications.

S. REP. NO. 99-541, at 38 (1994), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592.
327 *See supra* note 261.

> a device *or process* which records or decodes electronic or other impulses which identify the numbers dialed or otherwise *dialing, routing, addressing, or signaling information* transmitted on the telephone line to which such device is attached *by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication*, but such term does not include any device *or process* used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device *or process* used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business[.][328]

According to the Congressional Research Service,[329] section 216 was passed, in part, to,

> . . . update[ ] the language of the statute to clarify that the pen/ register authority applies to modern communication technologies. Current statutory references to the target "line," for example, are revised to encompass a "line or other facility." Such a facility includes: a cellular telephone number; [and] a specific cellular telephone identified by its electronic serial number (ESN) . . . . "Further, because the pen register or trap and trace 'device' is often incapable of being physically 'attached; to the target facility due to the nature of modern communication technology, [the] section . . . makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the section allows the pen register or trap

---

[328] 18 U.S.C. § 3127(3). This change was effectuated by section 216(c)(2) of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 290 (2001). Parenthetically note that a trap and trace "device," the conceptual opposite of a pen register, is defined at 18 U.S.C. § 3127(4) and was amended by section 216(c)(3) of the USA PATRIOT Act, in much a similar manner.

[329] "The Congressional Research Service is the public policy research arm of the United States Congress. As a legislative branch agency within the Library of Congress, CRS works exclusively and directly for Members of Congress, their Committees and staff on a confidential, nonpartisan basis." Congressional Research Sevice, http://www.loc.gov/crsinfo/whatscrs. html (last visited Apr. 7, 2007).

> and trace device to be 'attached or applied' to the target facility. Likewise, the definitions of 'pen register' and 'trap and trace device' in section 3127 [of Title 18] are revised to include an intangible 'process' (such as a software routine) *which collects the same information as a physical device."* [330]

It is important to recall that prior to the wireless revolution, the pen register was a mechanical instrument—a "physical device"—which was never capable of providing the telephone user's geographic location—not even roughly or approximately. The Pen/Trap Statute was amended to keep up with changing technology, to ensure that law enforcement would have access to the same or similar information—and not more[331]—in the burgeoning wireless environment as it had traditionally when wire communications were possible only in a hardline, copper wire, tangible instrument environment.

J. Precision GPS Tracking[332]

As noted briefly at the beginning,[333] GPS tracking permits greater precision (within meters) than is possible by only knowing which towers a cell phone is "hitting" (sometimes no better accuracy than within miles). As also pointed out, this more invasive[334] GPS tracking was judicially sanctioned in 2005 by a New York Federal District Court,

---

330 *Doyle*, *supra* note 291, at 12-13 (emphasis added).

331 E.g., location information.

332 > Global Positioning System (GPS), [is a] space-based radio-navigation system, consisting of 24 satellites and ground support. GPS provides users with accurate information about their position and velocity, as well as the time, anywhere in the world and in all weather conditions. GPS is available in two basic forms: the standard positioning service (SPS) and the precise positioning service (PPS). SPS provides a horizontal position that is accurate to about 100 m (about 330 ft); PPS is accurate to about 20 m (about 70 ft). For authorized users—normally the United States military and its allies—PPS also provides greater resistance to jamming and immunity to deceptive signals.

Microsoft ® Encarta ® Reference Library 2005.

333 *See supra* note 1.

334 I.e., relative to the degree of precision possible with most cell phone location/cell site results. Note that some Nextel phones have GPS capability: "GPS location-based safety services like Mobile Locator™, allows you to locate a friend or family member's phone location at anytime, right from your computer. Enjoy audible and visual turn-by-turn driving directions to any address, anywhere on Nextel's Nationwide Network. If you need to make a 911 emergency call, the GPS feature can also help emergency personnel locate you." *See* Nextel, http://nextelonline.nextel.com/NASApp/onlinestore/en/Action/SubmitRegionAction# drawers (last visited Apr. 7, 2007).

United States v. Moran[335] using a very uncomplicated *Knotts* analysis. In the absence of a warrant, a GPS device had been affixed to the defendant's vehicle; thereafter, at trial he moved to suppress all evidence derived therefrom. The court made the facile but now familiar observation that "[l]aw enforcement personnel could have conducted a visual surveillance of the vehicle as it traveled on the public highways."[336] As a consequence, the defendant "had no expectation of privacy in the whereabouts of his vehicle on a public roadway."[337] As a result, the judge remarked, it should not come as a surprise that "there was no search or seizure and no Fourth Amendment implications in the use of the GPS device."[338]

If no court order, and certainly not one grounded upon the Fourth Amendment, is needed to conduct relatively precise GPS tracking, it would therefore stand to reason that no probable cause order would be constitutionally required to obtain less accurate cell phone location information.

K. Change to Federal Rule of Criminal Procedure 41

By order dated April 12, 2006, the Supreme Court amended a number of Federal Rules of Criminal Procedure, including Rule 41, which became effective on December 1, 2006.[339] These rule changes, accompanied by excerpted notes from the Judicial Conference of the United States,[340] were transmitted on April 12, 2006 by the Chief Justice to both the Speaker of the House of Representatives and the President of the Senate.

Helpfully, the Judicial Conference Advisory Committee on Federal Rules of Criminal Procedure annotated the new changes with explanatory text which summarizes the changes to Rule 41. In sum, in those instances where a tracking device would implicate a Fourth Amendment "reasonable expectation" of privacy interest (such as

---

335 349 F. Supp. 2d 425 (N.D.N.Y. 2005).

336 *Id.* at 467.

337 *Id.*

338 *Id.*

339 Note that 28 U.S.C. § 2072(a) provides, in pertinent part, that "[t]he Supreme Court shall have the power to prescribe general rules of practice and procedure . . . for cases in the United States district courts (including proceedings before magistrate judges thereof)[.]"

340 *See* Adminisrative Office of the U.S. Court, Fed. R. Crim. P., Amend. Crim. R., Apr. 12, 2006, *available at* WL 2006 US Order 21; *see also* 28 U.S.C. § 331 (describing the judicial conference).

performing a hard-wire installation of a tracking device inside a vehicle trunk or monitoring the whereabouts of a motor vehicle located inside the garage of a private residence), an applicant—assuming there is sufficient evidence to establish probable cause[341]—may seek a Rule 41 tracking device warrant which permits monitoring for up to forty-five days after installation.[342] An unlimited number of extensions for up to 45 days each are permitted for "good cause" shown. The explanatory text makes clear that the new changes to Rule 41 are not meant to expand or contract the meaning of the term "tracking device" as set forth in 18 U.S.C. § 3117(b).[343] Installation must occur within ten calendar days (and during the daytime unless "good cause" to the contrary is shown) after the warrant is signed by the magistrate judge. Although installation of the "device" is to occur within the federal judicial district where the magistrate judge sits, the person or object being tracked may be monitored regardless of district.

Within ten calendar days after the tracking has been completed, the warrant's return must be made to the magistrate judge designated in the warrant. "The officer executing a tracking-device warrant must enter on it the exact date and time the device was installed and the period during which it was used."[344] A copy of the warrant, which serves as notice that the tracking has occurred, is to be provided to "the person who was tracked or whose property was tracked."[345]

> Service may be accomplished by delivering a copy to the person who, or whose property, was tracked; or by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address.[346]

---

341 If probable cause is demonstrated, the magistrate judge "must" issue the search warrant. This is unaltered from the version of Rule 41(d)(1) in effect prior to the change. Importantly, the explanatory text says that the Rule 41 modification does *not* "hold that such [tracking device] warrants may issue only on a showing of probable cause. Instead, it simply provides that if probable cause is shown, the magistrate judge must issue the warrant." FED. R. CRIM. P. 41 Advisory Comm. Nts. on the 2006 Amendments.

342 Any order would permit installation, needed maintenance/repair, monitoring, and any needed removal.

343 18 U.S.C. § 3117(b) (2000): "'[T]racking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object."

344 FED. R. CRIM. P. 41(f)(2)(A).

345 FED. R. CRIM. P. 41(f)(2)(C).

346 *Id.*

Such notice will, of course, probably compromise the investigation and thus it may be delayed "if the delay is authorized by statute,"[347] which, in this case, would be a reference to 18 U.S.C. § 3101(a). Section 3103(a), in turn, permits such a delay if the court finds "reasonable cause" to believe notice would otherwise occasion an "adverse result" (as defined at 18 U.S.C. § 2705).[348] The explanatory text also says that a delay "might be appropriate, for example, where the owner of the tracked property is undetermined . . . ."

IV. CONCLUSION

Although the success rate of DOJ's hybrid theory in support of cell site location information applications has been less than impressive, the only thing that is truly clear is that the state of the law is unclear. As of this writing,[349] only one of the USMJ cell site location opinions summarized above has been reviewed by a U.S. District Court Judge, nor does there appear to be any similar case (except *Forest*[350]) authored by higher judicial authority. This is bound to change, however, and readers should be alert as the law in this area continues to emerge.

---

347 FED. R. CRIM. P. 41(f)(3).

348 Incorporating 18 U.S.C. § 2705(a)(2), an "adverse result" would thus be defined as, (a) endangering the life or physical safety of an individual; (b) flight from prosecution; (c) destruction or tampering with evidence; (d) intimidation of potential witnesses; or (e) otherwise seriously jeopardizing an investigation.

349 November 6, 2006.

350 United States v. Forest, 355 F.3d 942 (6th Cir.), *cert. denied*, 543 U.S. 856 (2004).