UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN RE APPLICATION FOR PEN REGISTER	§	
AND TRAP/TRACE DEVICE WITH	§	MAGISTRATE NO. H-05-557M
CELL SITE LOCATION AUTHORITY	§	

OPINION

As part of an ongoing criminal investigation, the government seeks a court order compelling a cell phone company to disclose records of a customer's cell phone use. Among the records sought is "cell site data," which reveals the user's physical location while the phone is turned on. By order dated September 2, 2005, the court granted the application in large part, authorizing the continued use of a pen register/trap and trace device and disclosure of certain customer records including historical cell site data. However, the order denied access to prospective cell site information, for reasons explained more fully in this opinion.

The underlying order and application have been sealed at the government's request, in order not to jeopardize the ongoing criminal investigation. This opinion will not be sealed, because it concerns a matter of statutory interpretation which does not hinge on the particulars of the underlying investigation. The issue explored here has serious implications for the balance between privacy and law enforcement, and is a matter of first impression in this circuit as well as most others.[1]

Following its standard practice in this district, the government has combined its request for subscriber records with an application to install a pen register and trap/trace device on the target

---

[1] The only other reported decision on cell site data in this context is by Magistrate Judge James Orenstein, *In the Matter of Application of the United States for an Order Authorizing Pen Register and Trap and Trace Device and Release of Subscriber Information*, 384 F. Supp. 2d 562 (E.D.N.Y. Aug. 25, 2005). In *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004), the Sixth Circuit discussed the law enforcement technique of using cell phones as tracking devices in the context of a suppression motion.

phone. Basically, a pen register is a device or process which records the telephone numbers of outgoing calls; the trap and trace device captures the telephone numbers of incoming calls. *See* 18 U.S.C. § 3127. Among the most commonly used law enforcement techniques,[2] a pen/trap order authorizes real-time electronic monitoring of a telephone user's calls (excluding content) for a limited duration, typically 60 days. *Id.* at § 3123(c).

To assist this monitoring effort, the government seeks access to subscriber records maintained by the phone company pursuant to 18 U.S.C. § 2703(c). Among the records sought is "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." Sealed Application, at ¶ 21. Also sought is 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. Armed with this information, collectively known as "cell site data," investigators are often able to locate suspects and fugitives. The application makes this purpose explicit in a paragraph/sentence of clumsy boilerplate:

> [T]he device characteristics (such as model and capabilities), network characteristics (such as a provider's System and Base Identity listings, which are FCC assigned numbers used to identify providers and to subdivide their service markets, and communications protocol, e.g. GSM, CDMA, TDMA, or iDEN and Cellular vs. PCS service band), cell site listings (physical locations and numbering of towers), cell site activations and facings (when, and as, accessed by the **Target Device**), control channels and subchannels (the non-content communications signals that coordinate calls and help determine when a cell is switched or "handed-off"), signal strengths between the device and the cell site (used to estimate distance and determine when a cell site "hand-off" is necessary and possible), and other system information, when

[2] In this division alone, 313 pen register applications were processed in 2004. Through September 15 of the current year, 227 applications have been filed.

> coupled with the subscriber records for all calls identified by the pen register and trap and trace device may provide the general geographic location of the **Target Device** and, thus, may allow investigators to identify a suspect's location.

Sealed Application, at ¶ 20.

The issue presented here is what legal standard the government must satisfy to compel disclosure of such prospective or "real-time" cell site data. More particularly, is this location information 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 does this type of surveillance require a more exacting standard, such as probable cause under Federal Rule of Criminal Procedure 41?

1. Technology

Unavoidably, some familiarity with cell phone technology is necessary to address this issue. A cell phone is a sophisticated two-way radio with a low-power transmitter that operates in a network of cell sites.[3] "Cell" refers to geographic regions often illustrated as hexagons, resembling a bee's honeycomb; a "cell site" is where the radio transceiver and base station controller are located (at the point three hexagons meet). Cell phones and base stations communicate with each other on frequencies called channels. Two frequencies are paired to create a channel; one for transmitting, one for receiving. Channels that carry only cell system data are called control channels. The control channel is a frequency shared by the phone and the base station to communicate information for setting up calls and channel changing when the user moves from one cell to another. By comparison,

---

[3] For a general background on cellular telephones, see S. Rep. 99-541, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3563; see also Tom Farley, *Cellular Telephone Basics: AMPS and Beyond*, *at* http://www.privateline.com/Cellbasics/Cellbasics.html.

voice channels are those paired frequencies which handle a call's traffic, be it voice or data, as well as signaling information about the call itself. The cell site sends and receives traffic from the cell phones in its geographic area to a mobile telecommunications switching office, which handles all phone connections and controls all base stations in a given region.

When a cell phone is powered up, it acts as a scanning radio, searching through a list of control channels for the strongest signal. The cell phone re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed. The cell phone searches for a five-digit number known as the System Identification Code assigned to service providers. After selecting a channel, the cell phone identifies itself by sending its programmed codes which identify the phone, the phone's owner, and the service provider. These codes include an Electronic Serial Number (a unique 32-bit number programmed into the phone by the manufacturer), and a Mobile Identification Number, a 10-digit number derived from the phone's number.

The cell site relays these codes to the mobile telecommunications switching office in a process known as registration. The registration process is explained in the Department of Justice's Electronic Surveillance Manual:

> Cellular telephones that are powered on will automatically register or re-register with a cellular tower as the phone travels within the provider's service area. The registration process is the technical means by which the network identifies the subscriber, validates the account and determines where to route call traffic. **This exchange occurs on a dedicated control channel that is clearly separate from that used for call content (i.e. audio)–which occurs on a separate dedicated channel.**

U.S. Dep't of Justice, *Electronic Surveillance Manual*, at 178-79 n.41 (rev. June 2005)[4] (emphasis supplied).

---

[4] Posted on USABook Online, *available at* http://10.173.2.12/usao/eousa/ole/usabook/elsu.

It should be emphasized that cell site data transmitted during the registration process "are not dialed or otherwise controlled by the cellular telephone user." *Id.* at 40. This registration process automatically occurs even while the cell phone is idle. Moving from one service area to another triggers the registration process anew. The cell site can even initiate registration on its own by sending a signal to the cell phone causing the phone to transmit and identify itself.

When the switching office gets an incoming call, it sends a "page" to the cell phone over the control channel. When the cell phone responds, the switching office assigns a voice channel to carry the actual conversation; at that point the control channel drops off. The speaker's voice is converted into electronic digits (*i.e.* a series of 1s and 0s), which are then compressed for transmission over the voice channel.

In summary, a cell phone is (among other things) a radio transmitter that automatically announces its presence to a cell tower via a radio signal over a control channel which does not itself carry the human voice. By a process of triangulation from various cell towers, law enforcement is able to track the movements of the target phone, and hence locate a suspect using that phone.[5]

2. Statutes

The basic contours of electronic surveillance law were fixed by the Electronic Communications Privacy Act of 1986 ("ECPA"). Pub. L. No. 99-508, 100 Stat. 1848 (1986). The

---

[5] *See generally* Darren Handler, Note, *An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative*, 10 VA. J.L. & TECH. 1, at *8, *17-*21 (Winter 2005); Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-16 (Fall 2004).

ECPA comprised three titles. Title I amended the 1968 federal wiretap statute[6] to cover electronic communications. The Wiretap Act had imposed several additional requirements for lawful interception of a telephone conversation, beyond a judicial finding of probable cause: a wiretap is authorized only for specified crimes, for a limited duration, as a last resort, with minimized interception of innocent conversations, notice to targets, and extensive judicial oversight. *See generally* 18 U.S.C. § 2518. The ECPA amendments extended these restrictions to interception of electronic communications, with certain significant exceptions. This portion of the ECPA has no bearing on the issue before us, except to illustrate the full panoply of protections given to the content of private conversations under the Fourth Amendment; indeed, one commentator has referred to these wiretap requirements collectively as a form of "super-warrant." Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 630 (Winter 2003).

Another portion of ECPA's Title I concerns mobile tracking devices. Pub. L. No. 99-508, Title I, § 108(a), 100 Stat. 1858 (Oct. 21, 1986) (codified at 18 U.S.C. § 3117). The purpose of this provision was narrow: to authorize monitoring of tracking devices which may move across district lines. 18 U.S.C. § 3117(a). The ECPA was not intended to affect the legal standard for the issuance of orders authorizing these devices. *See* H.R. Rep. 99-647, at 60 (1986). A Rule 41 probable cause warrant was (and is) the standard procedure for authorizing the installation and use of mobile tracking devices. *See United States v. Karo*, 468 U.S. 705, 720 n.6 (1984) (warrantless monitoring of beeper in private residence violates Fourth Amendment); *United States v. Mixon,* 717 F. Supp.

---

[6] Commonly referred to as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Pub. L. No. 90-351, 82 Stat. 212 (codified at 18 U.S.C. § 2510-20) (the "Wiretap Act").

1169 (E.D. La.), *aff'd,* 891 F.2d 904 (5th Cir. 1989); *In re Application for Tracking Devices on a White Ford Truck*, 155 F.R.D. 401, 403 (D. Mass. 1994); *see also* J. CARR & P. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE § 4:83, at 4-199 (West 2004). Title I of the ECPA also defines the term "tracking device" to mean "an electronic or mechanical device which permits the tracking of the movement of a person or thing." 18 U.S.C. § 3117(b). This broad definition, which is cross referenced in other portions of the ECPA, carries important implications for cell site data access, to which we will return below.

Title II of the ECPA created a new chapter of the criminal code dealing with access to stored communications and transaction records. Pub. L. No. 99-508, 100 Stat. 1848, 1860 (1986) (codified at 18 U.S.C. § 2701 *et seq*.). This portion of the statute is commonly known as the "Stored Communications Act" or "SCA." The core is § 2703, authorizing government access to stored communications or transaction records in the hands of third party service providers. There are three categories of information, each with differing access requirements: (a) contents of wire or electronic communications in electronic storage; (b) contents of wire or electronic communications in a remote computing service; and (c) subscriber records concerning electronic communication service or remote computing service. The first two categories of content information generally require either a search warrant under Rule 41 or notice to the subscriber or customer. The third category of information–subscriber records–may be obtained by a court order upon proof of "specific and articulable facts showing ... 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). This

"specific and articulable facts" threshold, the result of a 1994 amendment, imposes an intermediate standard between an administrative subpoena and a probable cause warrant.[7]

Title III of the ECPA covers pen registers and trap/trace devices. Pub. L. No. 99-508, 100 Stat. 1848, 1873 (1986) (codified as amended at 18 U.S.C. §§ 3121-27). This portion of the Act will be referred to as the "Pen/Trap Statute." A "pen register" is a device that records the numbers dialed for outgoing calls made from the target phone.[8] A trap and trace device captures the numbers of calls made to the target phone. The Supreme Court held in *Smith v. Maryland*, 442 U.S. 735 (1979), that a person has no reasonable expectation of privacy in the telephone numbers she dials. Consequently, the legal hurdle for pen/trap surveillance is very low: a law enforcement officer need only certify that information likely to be obtained by the pen register or trap and trace device "is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b)(2). Upon that certification, the court must enter an *ex parte* order. 18 U.S.C. § 3123(a)(1), (2); *see also* J. CARR & P. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE § 1:26, at 1-25 (West 2004) ("In other words, the judge need not–and, indeed, cannot–independently assess the factual predicate for the government officials' certification").

---

[7] The SCA originally permitted access on a bare showing that there was "reason to believe . . . the records or other information sought, are relevant to a legitimate law enforcement inquiry." Pub. L. No. 99-508, Title II, § 201, 100 Stat. 1861 (Oct. 21, 1986). Congress tightened the standard by enacting the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), Pub. L. No. 103-414, Title II, § 207(a), 108 Stat. 4292 (Oct. 25, 1994), citing privacy concerns about the increasing amount of on-line transactional data compiled by service providers. H.R. Rep. No. 103-827(I), at 17, *reprinted at* 1994 U.S.C.C.A.N. 3489, 3497. The heightened standard was designed "to guard against 'fishing expeditions' by law enforcement." *Id.* at 31.

[8] The USA PATRIOT Act expanded the definition to cover not only dialing information but also addressing information for electronic communications. Pub. L. No. 107-56, § 216, 115 Stat. 272, 288 (2001).

Despite frequent amendment, the basic architecture of electronic surveillance law erected by the ECPA remains in place to this day. This statutory scheme has four broad categories, arranged from highest to lowest legal process for obtaining court approval:

- wiretaps, 18 U.S.C. §§ 2510-2522 (super-warrant);
- tracking devices, 18 U.S.C. § 3117 (Rule 41 probable cause);
- stored communications and subscriber records, 18 U.S.C. § 2703(d) (specific and articulable facts);
- pen register/trap and trace, 18 U.S.C. §§ 3121-3127 (certified relevance).

With this background in mind, we turn to the question at hand: what legal process is required for the government to collect prospective cell site data? In other words, which category of electronic surveillance law covers such location information?

3. <u>Prospective Cell Site Data as Tracking Information</u>

Our analysis begins with the tracking device category, which appears at first glance to provide the most likely fit for cell site location monitoring. In its first opinion dealing with the ECPA, the Fifth Circuit cautioned that rigorous attention must be paid to statutory definitions when interpreting this complex statute: "Understanding the Act requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis." *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994).

The ECPA's definition of tracking device is concise and straight-forward:

> As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or thing.

18 U.S.C. § 3117(b). Aside from its welcome brevity, the definition is striking for its breadth. Note that a device is covered even though it may not have been intended or designed to track movement;

it is enough if the device merely "permits" tracking. Nor does the definition suggest that a covered device can have no function other than tracking movement. Finally, there is no specification of how precise the tracking must be. Whether from room to room, house to house, neighborhood to neighborhood, or city to city, this unqualified definition draws no distinction.

The government contends that this interpretation of "tracking device" is too expansive, and points to the Senate Report on the ECPA which contained a glossary of technological terms defining "electronic tracking devices" as one-way radio "homing" devices. S. Rep. No. 541, 99th Cong., 2d Sess., at 10 (1986), *reprinted at* 1986 U.S.C.C.A.N. 3555, 3564. But even if this glossary definition accurately depicted the Senate's working understanding of the term in 1986, that definition never made it into the United States Code. So, if the government is correct that the glossary definition is narrower than § 3117(b), the only permissible inference is that Congress intended "tracking device" to have the broader meaning. Far from supporting the government's position, the glossary definition undermines it.

By adopting the broader language, Congress may simply have been anticipating future advances in tracking technology. Such advances have indeed come to pass:

> Tracking devices have progressed a long way. Most agencies now have sophisticated tracking devices **that use cell site towers** or satellites. . . . These types of tracking devices are usually monitored from the law enforcement agency's office. Through the use of computers, a signal is sent to the tracking device (it is pinged), and the tracking device responds. The signal is picked up **using cellular telephone cell sites** or satellites. The location of the tracker, and therefore the vehicle, is determined through triangulation and a computer monitor at the agency office shows the location of the vehicle on a map. These tracking devices are very accurate, and can differentiate between a vehicle traveling on an interstate highway or the feeder (service) road. The tracking devices will also provide the direction of travel and the speed the vehicle is traveling.

Robert Stabe, *Electronic Surveillance–Non-Wiretap*, § 3.31, *in* U.S. Dep't of Justice, *Federal Narcotics Prosecutions*.[9] (emphasis supplied). Thus, even traditional tracking devices such as beepers on vehicles are now monitored via radio signals using the very same cell phone towers used to transmit cell site data. Given this convergence in technology, the distinction between cell site data and information gathered by a tracking device has practically vanished. While Congress may not have known back in 1986 that a cell phone would come to be used as a tracking device, the broad language of § 3117(b) certainly left open that possibility.

While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data. As with a tracking device, this process is usually surreptitious and unknown to the phone user, who may not even be on the phone. The technique was described in *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004), where DEA agents lost visual contact with two individuals under wiretap surveillance for cocaine trafficking:

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

Id. at 947.[10] Garner's cell phone functioned no differently than a traditional beeper device, the only difference being that it was on his person instead of attached to his vehicle.

---

[9] Posted on USABook Online, *available at* http://10.173.2.12/usao/eousa/ole/usabook/drug/03drug.htm.

[10] The defendant moved to suppress, arguing that the DEA's use of his cell site data effectively turned his cell phone into a tracking device within the meaning of 18 U.S.C. § 3117. The court found it unnecessary to reach the issue because, whether or not this use of the cell phone met the definition of a tracking device, suppression was not an available remedy under that statute. *Id.* at 949-50.

The government resists categorizing cell site data in the hands of service providers as information from a tracking device, because it does not provide "detailed" location information. This argument is unpersuasive for several reasons. Textually, § 3117(b) does not distinguish between general vicinity tracking and detailed location tracking. Even if the statute had hinted at such a limitation, technological innovation would quickly render it obsolete. In December 1997, the Federal Communications Commission issued final "Enhanced 911" (E911) rules requiring cellular service providers to upgrade their systems to identify more precisely the longitude and latitude of mobile units making emergency 911 calls. By the end of 2005, carriers using handset-based location technology will be required to locate cell phones within 50 meters for 67% of calls, and 150 meters for 95% of calls. *See* 47 C.F.R. § 20.18(h) (2005). Location based services (LBS) are part of the next wave of cell phone features coming to the wireless marketplace. *See generally* David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, 8 COMM. L. & POL'Y 1 (Winter 2003). A recent Google search retrieved a website[11] advertising itself as a "leading provider of wireless location-based services (LBS) that leverage an individual's location to deliver customized, actionable information" such as "last known locations," "location-based alerts," and "proximity-based points of interest." This inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year.

The DOJ has not been so circumspect about applying the "tracking device" label in its own Electronic Surveillance Manual. Discussing an electronic device known as a "trigger-fish," which enables law enforcement to gather cell site data directly, without the assistance of the service

---

[11] *See* www.ulocate.com.

provider, the manual repeatedly uses the term "tracking device."[12] Yet the trigger-fish identifies the location of the user by exactly the same triangulation method that the government would apply to cell site data obtained from the cell phone company. If the tracking device label is warranted in the one case, it is warranted in the other. The label should not change merely because the equipment used to obtain the tracking data belongs to the service provider rather than law enforcement.

The government posits a slippery slope of adverse consequences unintended by Congress if cell phones could be classified as tracking devices under § 3117(b). For example, the government notes that land-line phones, computers, and even credit cards can sometimes reveal the user's location, and these things have never been considered tracking devices. But learning a credit card user's location at the point of purchase is far different from continuously monitoring a person's movement from place to place in real time. Section 3117(b) covers only those devices which permit the "tracking of the **movement** of a person or object." (emphasis supplied). Cell site data allows continuous tracking of actual movement, *i.e.*, change of location over time; the examples cited by the government do not.

In the same vein, the government argues that such a broad interpretation of § 3117(b) "would eviscerate privacy protection under the Wiretap Act and the SCA for most communications now

---

[12] In order to use such a device the investigator generally must know the target phone's telephone number (also known as a Mobile Identification Number or MIN). After the operator enters this information into the **tracking device**, it scans the surrounding airwaves. When the user of that phone places or receives a call, the phone transmits its unique identifying information to the provider's local cell tower. The provider's system then automatically assigns the phone a particular frequency and transmits other information that will allow the phone properly to transmit the user's voice to the cell tower. By gathering this information, the **tracking device** determines which call (out of the potentially thousands of nearby users) on which to home in. While the user remains on the phone, the **tracking device** can then register the direction and signal strength (and therefore the approximate distance) of the target phone.

U.S. Dep't of Justice, *Electronic Surveillance Manual*, at 44-45 (rev. June 2005) (emphasis supplied).

deemed electronic communications." Gov't Memorandum dated August 23, 2005, at 14. This argument rests on a fallacy– *i.e.*, that classifying cell site data as tracking information means that a cell phone must be regarded solely as a tracking device for all purposes, so that any form of communication from a cell phone *ipso facto* becomes a communication from a tracking device. Such reasoning ignores the multi-functional nature of the modern cell phone. This device delivers many different types of communication: live conversations, voice mail, pages, text messages, e-mail, alarms, internet, video, photos, dialing, signaling, etc. The legal standard for government access depends entirely upon the type of communication involved. Congress has decreed the highest protection for the contents of live conversations acquired via wiretap, intermediate protection for stored electronic communications, and the least protection for telephone numbers dialed. The legal threshold for each type of communication is different, notwithstanding that a cell phone transmits them all. It would surely make no sense to impose the wiretap requirements upon a pen/trap application merely because the cell phone can be used to intercept live conversations; it makes no more sense to impose the tracking device requirements for access to other types of cell phone communications unrelated to physical location.

Ironically, it is the government's position that threatens to undermine the federal statutory scheme for electronic surveillance. As we have seen, a cell phone can readily be converted by law enforcement to function as a tracking device, employing much the same technology as the modern beeper or transponder. Under the government's theory, law enforcement could simply install cell phones in place of the beepers currently underneath vehicles and inside drum barrels, and eliminate forever the need to obtain a Rule 41 search warrant for tracking surveillance. As explained more

fully in the next part, this would violate congressional intent by collapsing the barriers between the distinct categories of electronic surveillance erected by Congress in the ECPA.

A word about the Fourth Amendment implications of cell site tracking is in order here. The government contends that probable cause should never be required for cell phone tracking because there is no reasonable expectation of privacy in cell site location data, analogizing such information to the telephone numbers found unprotected in *Smith v. Maryland*, 442 U.S. 735 (1979). The Sixth Circuit rejected that analogy in *United States v. Forest*, 355 F.3d 942, 951-52 (6th Cir. 2004). Unlike 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. Sometimes, as in *Forest*, cell site data is triggered by law enforcement's dialing of the particular number. 355 F.3d at 951. For these reasons the Sixth Circuit was persuaded that *Smith* did not extend to cell site data, but rejected the defendant's constitutional claim on the narrower ground that the surveillance took place on public highways, where there is no legitimate expectation of privacy. *Id.* at 951-52 (citing *United States v. Knotts*, 460 U.S. 276, 281 (1983)).

Further support for a recognizable privacy interest in caller location information is provided by the Wireless Communication and Public Safety Act of 1999. Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct.26, 1999) (codified at 47 U.S.C. § 222(f)). This legislation authorized the deployment of a nation-wide 9-1-1 emergency service for wireless phone users, called "Enhanced 9-1-1." Section 5 of the bill amended the Telecommunications Act to extend privacy protection for the call location information of cell phone users:

(f) Authority to Use Wireless Location Information.–

> For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to–
>
> > (1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title), other than in accordance with subsection (d)(4) of this section; . . .

47 U.S.C. § 222(f). In other words, location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer. Based on this statute, a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.

For purposes of this decision it is unnecessary to draw the line between permissible and impermissible warrantless monitoring of cell site data. As in any tracking situation, it is impossible to know in advance whether the requested phone monitoring will invade the target's Fourth Amendment rights. The mere possibility of such an invasion is sufficient to require the prudent prosecutor to seek a Rule 41 search warrant. Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause.

4. <u>Prospective Cell Site Data and Other ECPA Surveillance Categories</u>

Having concluded that prospective cell site data is properly categorized as tracking device information under § 3117, the question arises whether such data may not also be obtainable under other provisions of the ECPA. In other words, do the four broad categories of the ECPA overlap, such that location information obtainable from a § 3117 tracking device is simultaneously obtainable

under the Wiretap Act, the SCA, or the Pen/Trap Statute? The answer to this question is clearly "no."

Two of the categories may be discarded at the outset. The minimal pen/trap standard does not authorize access to cell site data; Congress made that much clear in the Communications Assistance to Law Enforcement Act of 1994 ("CALEA"):

> [W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information **shall not include any information that may disclose the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).

47 U.S.C. § 1002(a)(2) (emphasis supplied).[13]

Nor is the super-warrant wiretap standard applicable here, because the government is not seeking to intercept the contents of a phone user's communication. Cell site data does not reflect the "contents" of a communication as that term is defined by the Wiretap Act. 18 U.S.C. § 2510(8) ("any information concerning the substance, purport, or meaning of that communication"). For the same reason, the first two parts of the SCA authorizing disclosure of the contents of stored communications do not apply, because the SCA incorporates the same definition of "contents." 18 U.S.C. § 2711(1). The only remaining possibility for prospective cell site data is the SCA subscriber records category under § 2703(c). The government's application understandably invokes this authority, with its lesser "specific and articulable facts" threshold. However, neither the text nor the structure of the SCA supports the government's contention.

---

[13] The government argues that recent amendments to the Pen/Trap Statute, when combined with section 2703(d) of the SCA, provide the necessary authority to compel disclosure of prospective cell site data. This "hybrid authority" argument is considered (and rejected) later in this opinion.

Carefully reviewing the language of the SCA, as *Steve Jackson* instructs, we find no mention of cell site data in the laundry list of basic subscriber information contained in § 2703(c)(2). The list does include "address," but this plainly refers to the subscriber's nominal residence for billing or contact purposes, rather than the physical location(s) where the mobile phone is used. In order to be accessible under the SCA, therefore, cell site data must fit within the broader category of transactional information referred to in § 2703(c)(1):

> **(c) Records concerning electronic communication service or remote computing service.–** (1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications).

The SCA does not define the term "record or other information pertaining to a subscriber or customer of such service," nor has any reported case interpreted the phrase. The legislative history is only slightly more helpful, noting that "the information involved is information about the customer's use of the service." S. Rep. No. 99-541, at 38, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592.

However, the ECPA does define other terms within § 2703(c)(1). The records to be disclosed must pertain to the subscriber's use of the provider's electronic communication service.[14] The term "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive *wire or electronic communications*." 18 U.S.C. §§ 2510(15), 2711(1) (emphasis added). The issue now becomes whether tracking device information, such as prospective cell site data, may constitute a record pertaining to "wire or electronic communications," as those

---

[14] For present purposes we may disregard "remote computing service," which refers to on-line activity such as e-mail.

terms are defined by the ECPA. If not, then access to such information is not authorized under the SCA.

Here at last the statute ceases to be so murky, yielding more definitive answers. Tracking device information such as cell site data is plainly not a form of electronic communication at all. "Electronic communication" is defined as follows:

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce, but **does not include–**
>
> * * *
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); . . .

18 U.S.C. § 2510(12)(C) (emphasis supplied). By virtue of this tracking device exclusion,[15] no communication from a tracking device can be an electronic communication. Real-time location monitoring effectively converts a cell phone into a tracking device, and therefore cell site data communicated from a cell phone is not an electronic communication under the ECPA.

The definition of "wire communication" does not contain a similarly explicit tracking device exclusion, but the answer is the same nevertheless. "Wire communication" is defined to mean a communication containing the human voice. *See* 18 U.S.C. §§ 2510(1), (18) (defining "wire communication" to be "any aural transfer" made in part through aid of wire, and defining "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and point of reception"). Cell site data is not a wire communication under this definition because it does not involve the transfer of the human voice at any point along the path between the

---

[15] This tracking device exclusion is applicable to all three titles of the ECPA: wiretaps, stored communications and transactional records, and pen/traps. 18 U.S.C. §§ 2510(12), 2711(1), and 3127(1).

cell phone and the cell tower. *United States v. Forest*, 355 F.3d 942, 949 (6th Cir. 2004) ("cell site data clearly does not fall within the definitions of wire or oral communication"). Although voice communications obviously do take place over a cell phone, this is accomplished on a channel or frequency entirely *separate* from the control channel that transmits the cell site data necessary to set up the call. U.S. Dep't of Justice, *Electronic Surveillance Manual*, at 178-79 n.41 (rev. June 2005). In fact, while the phone is on, cell site data is constantly transmitted over the control channel, even when the phone is not in use. *Id.* at 40.

To summarize, a communication from a tracking device, such as cell site data, is neither an electronic nor a wire communication under the ECPA, and so it does not fall within the range of covered services provided by an "electronic service provider." And since a subscriber does not use the phone to track his own movements in real time, prospective cell site data appears to be unrelated to any *customer* (as opposed to law enforcement) use of the provider's services. Thus, painstaking and methodical analysis of the SCA's technical terms offers no support for treating prospective cell site data as a transactional record under § 2703(c)(1).[16]

Even more compelling is the structural argument against allowing access to prospective cell site data under the SCA. Unlike other titles of the ECPA, which regulate methods of real-time surveillance, the SCA regulates access to records and communications in storage. As implied by its full title ("Stored Wire and Electronic Communications and Transactional Records Access"), the entire focus of the SCA is to describe the circumstances under which the government can compel disclosure of existing communications and transaction records in the hands of third party service

---

[16] By contrast, historical cell site data more comfortably fits the category of transactional records covered by the SCA. Cell phone companies might legitimately compile such data for customized marketing and billing purposes.

providers. Nothing in the SCA contemplates a new form of ongoing surveillance in which law enforcement uses co-opted service provider facilities.

Unlike wiretap and pen/trap orders, which are inherently prospective in nature, § 2703(d) orders are inherently retrospective. This distinction is most clearly seen in the duration periods which Congress mandated for wiretap and pen/trap orders. Wiretap orders authorize a maximum surveillance period of 30 days, which begins to run no later than 10 days after the order is entered. 18 U.S.C. § 2518(5). Pen/trap orders authorize the installation and use of a pen register for a period "not to exceed sixty days." 18 U.S.C. § 3123(c)(1). By contrast, Congress imposed no duration period whatsoever for § 2703(d) orders. Likewise, Congress expressly provided that both wiretap orders and pen/trap orders may be extended by the court for limited periods of time. 18 U.S.C. §§ 2518(5), 3123(c)(2). There is no similar provision for extending § 2703(d) orders. Pen/trap results are ordinarily required to be furnished to law enforcement "at reasonable intervals during regular business hours for the duration of the order." 18 U.S.C. § 3124(b). The wiretap statute authorizes periodic reports to the court concerning the progress of the surveillance. 18 U.S.C. § 2518(6). Again, nothing resembling such ongoing reporting requirements exists in the SCA.

Another notable omission from § 2703(d) is sealing of court records. Wiretap orders and pen/trap orders are automatically sealed, reflecting the need to keep the ongoing surveillance under wraps. 18 U.S.C. §§ 2518(8)(b), 3123(d)(1). The SCA does not mention sealing. Pen/trap orders must also direct that the service providers not disclose the existence of the order to third parties until otherwise ordered by the court. 18 U.S.C. § 3123(d)(2). Section 2705(b) of the SCA authorizes the court to enter a similar non-disclosure order, but only upon a showing of possible adverse

consequences, such as "seriously jeopardizing an investigation or unduly delaying a trial." 18 U.S.C. § 2705(b)(1)-(5).

Taken together, the presence of these provisions in other titles of the ECPA and their corresponding absence from the SCA cannot simply be dismissed as a coincidence or congressional absent-mindedness. Pen registers and wiretaps are surveillance techniques for monitoring communications yet to occur, requiring prior judicial approval and continuing oversight during coming weeks and months; § 2703(d) permits access to customer transaction records currently in the hands of the service provider, relating to the customer's past and present use of the service. Like a request for production of documents under Federal Rule of Civil Procedure 34, § 2703(d) contemplates the production of existing records, not documents that may be created at some future date related to some future communication. That is the most obvious explanation why the SCA makes no mention of surveillance periods, extensions, periodic reporting, or sealing. If Congress had not intended the SCA to be retrospective in nature, it would have included the same prospective features it built into the wiretap and pen/trap statutes.

5. <u>The Government's Hybrid Theory</u>

The Sealed Application does not cite the Pen/Trap Statute as authority for obtaining cell site data, for good reason. As noted previously, CALEA explicitly prohibits service providers from disclosing cell phone location information in response to a pen/trap order. 47 U.S.C. § 1002(a)(2). The only other reported decision on cell site data has held that this portion of CALEA forbids law enforcement from obtaining cell site location under a pen/trap order. *In the Matter of Application*

of the United States for an Order Authorizing the Use of a Pen Register and Trap and Trace Device and Authorizing Release of Subscriber Information, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).

The government nevertheless contends that a pen/trap order, when combined with a § 2703(d) order, is sufficient authority to collect prospective cell site data. This dual or "hybrid" authority argument is based on a subtle concatenation of three different statutes. The argument proceeds as follows: (1) prospective cell site data falls within the PATRIOT Act's expanded definitions of "pen register" and "trap and trace device"[17] because carriers use cell site data for "routing" calls to and from their proper destination; (2) CALEA amended the law to prevent disclosure of a caller's physical location "solely" pursuant to a pen/trap order, so the government need only have some additional authority besides the Pen/Trap Statute to gather prospective cell site information; (3) the SCA provides that additional authority, because cell site data is non-content subscriber information obtainable upon a "specific and articulable facts" showing under § 2703(d); and (4) completing the circle, cell site data authorized by a § 2703(d) order may be collected *prospectively* by virtue of the forward-looking procedural features of the Pen/Trap Statute. 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.

---

[17] *See* 18 U.S.C. §§ 3127(3), (4), defining these terms as devices or processes which record or capture "dialing, routing, addressing, or signaling information."

Initially, it must be observed that the text of neither the Pen/Trap Statute nor the SCA mentions such hybrid treatment for cell site data. The government's construction of congressional silence might nevertheless be reasonable, assuming its premises were valid. However, those premises do not withstand careful scrutiny.

First, the PATRIOT Act's expansion of pen/trap definitions was intended only to reach electronic communications such as e-mail. The added term "dialing, routing, addressing, and signaling information," while not defined in the statute, was touted by the bill's proponents as a way to update the pen/trap statute to cover Internet traffic. *See* 147 Cong. Rec. S11006-07 (Oct. 25, 2001) (statement of Sen. Leahy); 147 Cong. Rec. H7197 (Oct. 23, 2001) (statement of Rep. Conyers). Nothing in the admittedly abbreviated legislative history of the PATRIOT Act suggests that this new definition would extend the reach of the Pen/Trap Statute to cell phone tracking. Contemporary summaries of the PATRIOT Act prepared by knowledgeable commentators, including the DOJ itself, make no mention of expanding pen/traps to capture cell site data.[18] Surely, even amidst the other important features of that broad-ranging statute, such an important change in electronic surveillance law would have been noticed by *someone*.

Nor is it certain that the new definition actually encompasses the cell site data now sought by the government. The traditional pen register was triggered only when the user dialed a telephone

---

[18] *See* U.S. Dep't of Justice, *Computer Crime and Intellectual Property Section: Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (noting that "Section 216 [of the Patriot Act] updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider." *See also* Robert Stabe, *Electronic Surveillance–Non-Wiretap*, § 3.4, *in* U.S. Dep't of Justice, *Federal Narcotics Prosecutions*; *American Civil Liberties Union: Surveillance Under the USA Patriot Act*, *available at* http://www.aclu.org/news/NewsPrint.cfm?ID=12263&c=206.

number; no information was recorded by the device unless the user attempted to make a call. The PATRIOT Act clarified that a pen register could also record "routing, addressing, and signaling information," as well as numbers dialed. But the expanded definition also indicates that this "routing, addressing, and signaling" information is generated by, and incidental to, the transmission of "a wire or electronic communication." 18 U.S.C. § 3127(3). In other words, today's pen register must still be tied to an actual or attempted phone call.[19] As we have already seen, much cell site data is transmitted even when the user is not making or receiving a call, *i.e.*, when no wire or electronic communication is transmitted. In short, neither the text nor the legislative history of the PATRIOT Act offer much support for the government's contention that the cell site data it seeks is covered by the new pen/trap definitions.

The government's second premise, that the CALEA proviso was intended to amend existing law, is refuted by its legislative history. One of CALEA's main objectives was to allow law enforcement to retain existing surveillance capabilities in the face of technological change in the telecommunications field. *See generally* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949 (1996). This goal was to be accomplished by, among other things, requiring telecommunications companies to ensure that its equipment would be capable of "enabling the government, pursuant to a court order or other lawful authorization, to access **call-identifying information** that is reasonably available to the carrier."

---

[19] The House Report on the bill that became the PATRIOT Act notes that "orders for the installation of pen register and trap and trace devices may obtain any non-content information– 'dialing, routing, addressing, and signaling information'– *utilized in the processing or transmitting of wire and electronic communications.*" H.R. Rep. No. 236(I), 107th Cong. 1st Sess., at 53 (2001) (emphasis supplied).

Pub. L. No. 103-414, Title I, § 103, 108 Stat. 4280 (Oct. 25, 1994) (codified at 47 U.S.C. § 1002(a)(2)) (emphasis supplied).

This assistance proposal was challenged before passage by some privacy advocates, who worried that the broad definition of call-identifying information would be construed as amending the pen register statute to authorize tracking of cell phone users under that statute's minimal requirements. To allay such concerns, FBI Director Louis Freeh, the most vigorous proponent of the legislation, forcefully testified that the proposed legislation "ensures the maintenance of the status quo" as to the legal authority for wiretaps and pen/traps, that the bill "does not enlarge or reduce the government's authority" for such electronic surveillance, and that the proposed legislation "relates solely to advanced technology, not legal authority or privacy." *See Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings Before the Subcomm. on Technology and Law of the Senate Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm.*, 103rd Cong., 2d Sess., at 2, 28 (statement of Director Freeh).

Director Freeh was particularly keen to defuse what he described as a false "transactional data scare" that the government was "seeking to 'dictate to industry' a new capability to acquire 'minute by minute surveillance of individuals' through transactional data." *Id.* at 27. He testified:

> This is a false issue for a number of reasons. First, . . . the intent of the legislation is to maintain existing technical capabilities and to "clarify and define the responsibilities of common carriers . . . to provide the assistance required to ensure that government agencies can implement court orders and lawful authorizations to intercept the content of wire and electronic communications and acquire call setup information under chapters 119 and 206 of Title 18 and chapter 36 of Title 50." (emphasis added). **These chapters have nothing to do with "transactional information" under our federal electronic surveillance and privacy laws. All telecommunications "transactional" information is already protected by federal**

> **law and is exclusively dealt with in chapter 121 of Title 18 of the United States Code ("Stored Wire and Electronic Communications and Transactional Records Access"). The proposed legislation does not relate to chapter 121 of Title 18.** Second, under federal law, Congress treats law enforcement's use of pen registers and dialing information differently than "transactional information"–such as detailed telephone billing information. . . .

Id. at 27-28 (emphasis supplied).

In order to dispel all doubt about law enforcement intentions, the FBI director proposed inserting the clarifying disclaimer, which eventually was incorporated into the statute at 47 U.S.C. § 1002(a)(2) ("information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber"). *Id.* at 29. Significantly, the effective date of this proviso was to be four years after enactment, the same time the assistance capability provisions became effective. *See* Pub. L. 103-414, § 111(b). By contrast, other portions of CALEA, including the "specific and articulable facts" standard for § 2703(d), were effective on the date of enactment, October 25, 1994. *Id.* at § 111(a).

This legislative history undermines the CALEA step in the government's hybrid authority argument. Rather than altering federal surveillance law, the disclaimer of pen/trap authority was intended to assure that the existing legal framework would continue to apply **in spite of** anticipated technological advances, at least with respect to physical location information. While the disclaimer did not affirmatively specify what legal authority would govern access to prospective cell site data, Director Freeh's testimony makes clear that an order under SCA § 2703(d) was not a likely suspect. *Id.* at 28 ("The proposed legislation does not relate to chapter 121 of Title 18"). Far from the silent synergy of disparate statutes now posited by the government, the FBI director in 1994 was insisting that the Pen/Trap Statute has "nothing to do with" the SCA, and that transactional information "is

exclusively dealt with in chapter 121 of Title 18," *i.e.*, the SCA. *Id.* at 27-28. Congress unquestionably placed great weight upon the testimony of the FBI Director, law enforcement's chief spokesman and leading advocate for the bill. *See, e.g.*, H.R. Rep. No. 103-827(I), *reprinted in* 1994 U.S.C.C.A.N. 3489, at 24 ("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"). Given Director Freeh's disclaimer, it is highly unlikely that Congress intended CALEA to expand law enforcement surveillance powers in the manner now suggested by the government.

The government's third premise, that § 2703(d) authorizes collection of prospective cell site data has already been considered and rejected above in part 4.

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

paternity somewhere along the way.[20] This is especially so given that no other form of electronic surveillance has the mixed statutory parentage that prospective cell site data is claimed to have.

Besides a doubtful pedigree, there is also uncertainty about the hybrid's birthday. These statutes were passed at various times over a 15-year period (1986 to 2001). If as the government contends all three statutes were necessary for conception, then the statutory authority for this surveillance technique was obviously born after the PATRIOT Act amendments of 2001. But this timing undercuts any inference that the CALEA proviso (passed 1994, effective 1998) authorized disclosure of location information under the SCA "specific and articulable facts" standard. What need of subsequent legislation if CALEA already did the trick? On the other hand, if CALEA itself marked the true birth date, then the expanded pen/trap definitions in the subsequent PATRIOT Act are rendered immaterial to the analysis. But without the expanded pen/trap definitions, there is no basis to argue that the Pen/Trap Statute covered cell site data; the old definitions only covered

---

[20] In July 2000, six Republican congressmen introduced a bill (H.B. 5018) which would have amended the SCA to require a probable cause showing by the government to gain access to cell phone location information. The bill, entitled the Electronic Communications Privacy Act of 2000, was intended to remedy the perceived lack of "clear legal standards governing when the government can collect location information from cell phone companies." H. Rep. 106-932, 106th Cong., 2d Sess. Oct. 4, 2000, *reprinted at* LEXSEE 106 H. Rep. 932, at 15. Although favorably reported out of committee, the bill was never brought to a vote on either the House or Senate floor, and died a natural death at the close of the Clinton administration. Inchoate legislation (such as H.B. 5018) never presented to either house of Congress is practically meaningless as legislative history for statutes actually enacted by another Congress. *See NLRB v. Health Care & Retirement Corp. of America,* 511 U.S. 571, 582 (1994); *Pension Benefits Guaranty Corp. v. LTV Corp.*, 496 U.S. 633, 649-50 (1990) ("It is a particularly dangerous ground on which to rest an interpretation of a prior statute when it concerns, as it does here, a proposal that does not become law"); *United States v. Wise*, 370 U.S. 405, 411 (1962) ("Logically, several equally tenable inferences could be drawn from the failure of Congress to adopt an amendment in light of an interpretation placed upon existing law by some of its members, including the inference that existing legislation already incorporated the offered change"); *see also United States v. Guerlain, Inc.*, 155 F. Supp. 77, 82 (S.D.N.Y. 1957), *vacated on other grounds*, 358 U.S. 915 (1958) ("If the failure of enactment of every amendment offered for consideration of Congress were necessarily held to shed light on the legislation sought to be amended, the search for Congressional intention would be endless and fruitless"). The demise of H.B. 5018 sheds no light on the cell site location issue.

numbers dialed.[21] And without the Pen/Trap Statutes's prospective features, so clearly lacking in the SCA scheme, the statutory underpinnings for monitoring of cell phone location simply collapse.

6. Conclusion

The government's hybrid theory, while undeniably creative, amounts to little more than a retrospective assemblage of disparate statutory parts to achieve a desired result. Viewing each statute in proper temporal perspective, there is simply no reason to believe that Congress intended to treat location monitoring of cell phones as an exceptional type of electronic surveillance. While Congressional enactments are sometimes difficult to decipher, employing such a three-rail bank shot to create a new category of electronic surveillance seems almost perverse. Had Congress truly intended such an outcome, there were surely more direct avenues far less likely to confound and mislead judicial inquiry.

Denial 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. On the other hand, permitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected. *Cf. United States Telecom Ass'n v. FCC*, 227 F.3d 450, 464 (D.C. Cir. 2000) (citing with approval an FCC finding that providing law enforcement with triangulation capability from cell site towers "poses difficulties that could undermine individual privacy"). Absent any sign that Congress has squarely addressed and resolved those concerns in

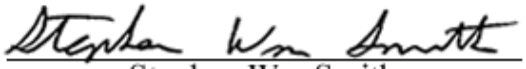
---

[21] *See* Pub.L. 99-508, Title III, § 301(a), 100 Stat. 1871, 1872 (Oct. 21, 1986).

favor of law enforcement, the far more prudent course is to avoid an interpretation which risks a constitutional collision.

Judge Orenstein's opinion was the first word on this topic; this opinion will undoubtedly not be the last. It is written in the full expectation and hope that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis.

Signed on October 14, 2005, at Houston, Texas.



Stephen Wm Smith
United States Magistrate Judge