PREVENTING A MODERN PANOPTICON: LAW ENFORCEMENT ACQUISITION OF REAL-TIME CELLULAR TRACKING DATA

Steven B. Toeniskoetter*

Cite as: Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 RICH. J.L. & TECH. 16 (2007), http://law.richmond.edu/jolt/v13i4/article16.pdf.

I. INTRODUCTION

[1] Nineteenth Century philosopher Jeremy Bentham designed a prison system known as the Panopticon which was arranged in such a way that a single guard could, at any given time, view the activities and whereabouts of any particular prisoner.[1] Bentham designed the prison in such a way that the prisoners could never tell whether they were being watched.[2] Twentieth Century French philosopher Michel Foucault further considered use of the Panopticon as a means of societal control through fear in his seminal book *Discipline and Punish: The Birth of the Prison*.[3] Foucault viewed the Panopticon as representative of society's change in the Eighteenth Century from a power structure which exercised control through public spectacle (e.g., public hangings and torture) to one which

*Steven B. Toeniskoetter earned his J.D., *cum laude*, from the University of San Francisco School of Law in 2006. He would like to thank Professor Susan Freiwald for bringing this issue to his attention and providing comments and critiques on early drafts.

[1] James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997); Wikipedia, *Panopticon Definition*, *available at* http://en.wikipedia.org/wiki/Panopticon (last visited May 09, 2007). Panopticon literally means the "all-seeing", from the ancient Greek word πανόπτης.

[2] *Id.*

[3] MICHEL FOUCAULT, DISCIPLINE AND PUNISH 195-228 (Alan Sheridan, trans., Vintage Books 2d ed. 1995) (1977).

exercised control through constant, unseen surveillance.[4] Cellular tracking data has the potential to function as a Panopticon – permitting a single entity to monitor the location (and thereby the activities) of any particular person without that person ever knowing. Cellular tracking technology presents many potentially advantageous uses, not the least of which is the ability to track down a user during an emergency situation. But like any powerful and invasive technology, the potential for abuse is also great. Government and private actors could use cellular tracking technology to track the movements of political opponents, members of unpopular groups, or every citizen in the country and ultimately control their activities through the fear of constant surveillance. Current electronic surveillance law permits this type of abuse because of the lack of proper constraints on law enforcement's acquisition of prospective cell site data.

[2] New communications technology has always posed classification and regulation problems for courts and legislators; cellular technology is no exception. When Congress originally enacted the Electronic Communications Privacy Act of 1986 (ECPA),[5] cellular technology was in its infancy and the ability to track users via their cellular telephones was rudimentary at best. Congress could not have foreseen at the time that cellular technology could eventually be used to track individuals with the substantial accuracy now available.

[3] Since the passage of the ECPA, a confusing patchwork (or "mosaic" according to one court[6]) of laws regulating cellular technology has emerged. Courts have split on whether to permit government agents access to real-time cellular tracking information ("prospective cell site data") pursuant to a "hybrid theory"[7] application.

---

[4] Several authors have sought to apply Foucault's ideas on surveillance to online and electronic surveillance. *See, e.g.,* Mark Winokur, *The Ambiguous Panopticon: Foucault and the Codes of Cyberspace*, CTHEORY.NET ONLINE JOURNAL, *available at*: http://www.ctheory.net/articles.aspx?id=371; Boyle *supra* note 1.

[5] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2703 (2006).

[6] *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006) [hereinafter Wisconsin Decision].

[7] The "hybrid theory" application refers to an application for prospective cell site data based upon the combined authority of a pen register order with that of a Stored Communications Act order. *See infra* Section IV.

[4] This paper first discusses current cellular technology and related regulation in Section II. Section III provides an overview of the statutes that govern cellular tracking technology and the cases that applied these statutes prior to 2005. Section IV discusses recent cases that address the procedural standard applicable to government acquisition of prospective cell site data. Section V contains my analysis of the statutory and constitutional framework applicable to law enforcement acquisition of prospective cell site data. Section VI argues that Congress should fix the ambiguities in the law to provide certainty and security for cellular users and to prevent potential abuse of cell site data.

II. CELLULAR TRACKING TECHNOLOGY

[5] In order to evaluate the standards governing the acquisition of prospective and real-time cellular tracking data (hereinafter "prospective cell site data"[8]), it is necessary to first examine what sort of location data the government has used cell phone technology to obtain. Unfortunately there is no definitive answer. The court decisions addressing the issue are either unclear about what the government has actually been able to obtain or they contradict each other. However, based upon the facts of several court decisions, the Enhanced 911 legislation (E-911), and several other materials, it appears that the government can obtain data that fairly accurately identifies the location of cell phone users. An examination of the FCC's Wireless Enhanced 911 service reveals the capabilities of current technology.

A. ENHANCED 911 RULES

[6] In 1996, the FCC began creating rules to ensure that cellular phone users would be able to connect to 911 operators through their cellular phones and that the 911 operators would be able to obtain the location of the cellular phone directly from the cellular service provider. The E-911 regulations, which are to be promulgated over time, require cellular service providers to provide certain minimum pieces of information to 911

[8] The courts discussing this issue use both the term "prospective cell site data" and "real-time cell site data." As one court has discussed, the terms are not interchangeable. *See* Section IV(C), *infra*. I generally use the term "prospective cell site data" for this paper since "real-time cell site data" is a sub-category of prospective cell site data.

operators.[9] In Phase I, which required implementation by April 1, 1998, cellular service providers were required to provide 911 operators with the location of the single "cell site or base station" which received the 911 call.[10] The cellular service providers merely had to provide the location of a single cellular tower, and emergency responders would know the cellular phone was within a certain radius of that cellular tower. Factual recitations in recent court decisions reveal that at least some cellular providers also have the ability to provide the general direction and/or angle the cellular phone is in relation to the cell site.[11] For ease of reference, I will refer to this type of location data as "single cell site data."

[7] In Phase II, the FCC required cellular service providers to provide 911 operators with the location of a cellular phone by longitude and latitude.[12] The E-911 regulations provide two ways of meeting this requirement: network-based technologies and handset-based technologies. Providers who decided on network-based technologies had to ensure accuracy of within 100 meters for sixty seven percent of calls and within 300 meters for 100 percent of calls by October 1, 2002.[13] Providers who decided on handset-based technologies had to ensure accuracy of within fifty meters for sixty seven percent of calls and within 150 meters for ninety five percent of calls by October 1, 2001.[14]

[8] The term "network-based technologies" refers to the use of triangulation to determine the general location of a cellular phone. Network-based technologies require that two or more cell towers receive a signal or signals from a cellular telephone at or about the same time.[15]

---

[9] 47 C.F.R. § 20.18 (2006).
[10] 47 C.F.R. § 20.18(d)(1).
[11] *See, e.g., In Re* Application Of The United States of America For An Order For Disclosure Of Telecommunications Records And Authorizing The Use Of A Pen Register And Trap And Trace, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005) (Gorenstein, M.J.) [hereinafter S.D.N.Y. I]; *Wisconsin Decision*, 412 F. Supp. 2d at 950.
[12] 47 C.F.R. § 20.18(e).
[13] 47 C.F.R. § 20.18(f) & (h).
[14] 47 C.F.R. § 20.18(g) & (h).
[15] Where only one cell tower has received a signal from a cellular telephone, the data provided is essentially single cell site data (i.e. a certain radius around a single cell tower). For a more in-depth discussion of the different types of triangulation and a general discussion of E-911, see Darren Handler, Comment, *An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative*, 10 VA.

Several recent court decisions reveal that in addition to the location of a single cell site, such data may also reveal which general direction and/or angle the cellular phone is in relation to the cell site.[16] The accuracy of triangulation techniques generally improves with each additional cell phone tower that receives a signal at about the same time. Consequently, triangulation technology is most effective in urban areas where cell tower density is high and much less effective in rural areas where cell tower density is low.[17]

[9] The term "handset-based technologies" at this time seems to refer solely to GPS-based[18] systems for determining the location of a cellular telephone. A cellular provider using a GPS-based system uses a GPS receiver built in to the cellular phone handset itself to obtain the handset's location, which is then transmitted to the 911 operator.[19] Normal GPS accuracy is approximately within four to twenty meters, but that accuracy can be improved using several additional technologies to within ten centimeters.[20] In contrast to triangulation technology, GPS tends to be *more* accurate in rural areas than in urban areas because the signal can be distorted by large buildings.[21]

J.L. & TECH. 1 (2005); *Recent Development*, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-10 (2004) [hereinafter *Who Knows Where You've Been*]; Laurie Thomas Lee, *Can Police Track Your Wireless Calls? Call Location Information and Privacy Law*, 21 CARDOZO ARTS & ENT. L.J. 381, 384-88 (2003). *See also* Wikipedia, Radiolocation Definition, http://en.wikipedia.org/wiki/Radiolocation (last visited May 9, 2007) (describing the types of triangulation each major cellular provider currently uses).

[16] *See* note 10 *supra* and accompanying text..

[17] One article has suggested there may be areas in which a single cell tower covers an area of several hundred miles. *Who Knows Where You've Been supra* note 15, at 309.

[18] GPS, which stands for Global Positioning System, is a U.S. Government-developed satellite system for determining a receiver's location anywhere on earth. *See generally*, Wikipedia, GPS Definition, http://en.wikipedia.org/wiki/GPS (last visited May. 9 2007) [hereinafter Wikipedia GPS Definition].

[19] *See* 911 Dispatch Monthly Magazine Online, GPS Location Technology Page, http://www.911dispatch.com/911/gps.html (last visited May 9, 2007).

[20] Wikipedia, GPS Definition, *supra* note 18.

[21] *Id.* This effect is called an "urban canyon." However, in major urban centers, this effect is lessened by the use of stationary GPS reference points called Wide Area Augmentation Systems. *See* Wikipedia, Wide Area Augmentation System Definition, http://en.wikipedia.org/wiki/Wide_Area_Augmentation_System (last visited May 9, 2007).

B. TYPES OF CELL SITE DATA AND THEIR AVAILABILITY

[10] The E-911 legislation reveals that there are three types of cellular tracking data that government agents can potentially obtain from cellular providers.

[11] In order from the most accurate to least accurate they are:

(1) GPS data
(2) Triangulation data
(3) Single cell site data.[22]

[12] There are eight times at which each type of data could be available:

(1) Whenever a cellular phone is turned on
(2) At the beginning of an outbound call
(3) At the beginning of an inbound call
(4) During an inbound or outbound call
(5) At the end of an outbound call
(6) At the end of an inbound call
(7) At the beginning of a 911 call
(8) At any time during a 911 call.[23]

[13] It is unclear exactly when a cellular provider can itself obtain any of these three types of data. For instance, the E-911 regulations merely require the cellular providers to provide GPS data when a cell phone user dials 911.[24] It is unclear whether the provider may obtain and record GPS data whenever the cell phone is on or only while that person is on the phone with a 911 operator.[25] In several recent court decisions, the Assistant U.S. Attorney's (AUSA's) application seeks tracking data only

[22] *See generally* 18 U.S.C. § 2703 (2006); Lee *supra* note 15.
[23] *Id.*
[24] 47 C.F.R. § 20.18(e).
[25] Some cellular phones with GPS allow users the ability to turn off the GPS for all purposes but 911 service. *See, e.g.,* Sprint PCS Website, Sanyo 8200 User's Guide at 65, *available at* http://www1.sprintpcs.com/media/Assets/Equipment/Handsets/pdf/sanyopm8200.pdf (last visited May 9, 2007).

at the beginning and end of calls[26] while in several other court decisions, the AUSA seeks tracking data during a call as well.[27]

III. THE LAW PRE-2005

A. INTRODUCTION

[14] An examination of the law prior to recent decisions reveals the building blocks upon which the latest court decisions rest. Accordingly, this section reviews the existing federal statutory scheme governing wiretapping, pen registers, stored electronic data, and tracking devices, as well as Fourth Amendment case law as it applies to tracking devices.

B. WIRETAP ACT AND ITS PROGENY

[15] In 1967, the Supreme Court in *Katz v. United States* (hereinafter *Katz*) broke new ground by finding that law enforcement agents needed a warrant before they could listen to a person's telephone conversations.[28] The *Katz* court held that "the Fourth Amendment protects people – and not simply 'areas….'"[29] The Court, through a concurring opinion, adopted a new test for when communications would be protected under the Fourth Amendment: Whenever a defendant exhibited a subjective expectation of privacy in the communications and when that expectation of privacy is

[26] *See, e.g*., S.D.N.Y. Decision I, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); Wisconsin Decision, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re* Application Of The United States For An Order: (1) Authorizing The Installation & Use Of A Pen Register & Trap & Trace Device; & (2) Authorizing Release Of Subscriber Info. &/Or Cell Site Info., 411 F.Supp.2d 678 (W.D. La. 2006) (Hornsby, M.J.) [hereinafter Louisiana Decision].

[27] *See, e.g., In* re Application for Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F.Supp.2d 747 (S.D. Tex. 2005) [hereinafter Texas Decision]; *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Information &/or Cell Site Info. (E.D.N.Y. Decision I), 384 F.Supp. 2d 562 (E.D.N.Y. 2005); *on reconsideration* (E.D.N.Y. Decision II), 396 F.Supp. 2d 294, 327 (E.D.N.Y. 2005). For the purposes of this paper, I treat E.D.N.Y. Decisions I and II as the same decision.

[28] Katz v. United States, 389 U.S. 347 (1967).

[29] *Id*. at 353.

objectively reasonable.[30] The *Katz* court acknowledged the "vital role that the public telephone has come to play in private communication."[31]

[16] Within one year of the *Katz* decision, and in direct response to that decision, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (commonly referred to as the "Wiretap Act").[32] The Wiretap Act generally forbade private parties from intercepting any covered communications, except with consent of the parties, and required law enforcement agents to follow strict procedural requirements in order to intercept wire communications.[33]

[17] In response to another technological revolution, the proliferation of electronic mail, voicemail, and cordless and cellular telephones, Congress passed the Electronic Communications Privacy Act of 1986 (ECPA).[34] Title I extended most of the protections of the Wiretap Act to electronic communications, [35] Title II added a new section protecting stored communications and transactional records (known as the "Stored Communications Act" (SCA)), and Title III added a new section on pen registers and trap and trace devices ("Pen Register Provisions").[36]

1. STORED COMMUNICATIONS ACT

[18] The SCA regulates how government agencies may obtain transactional records and communications which have been stored electronically (i.e., communications obtained in a manner not simultaneous with their transmission).[37] What follows is a distillation of

[30] *Id.* at 361. (Justice Harlan, concurring).
[31] *Id*. at 352.
[32] Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified at 18 U.S.C. §§ 2510-2520) (2000)).
[33] *Id*.
[34] Pub. L. No. 99-508, 100 Stat. 1848 (1986).
[35] While ECPA Title I generally extended the Wiretap Act to cover electronic communications, it explicitly exempts electronics communications from the statutory suppression remedy available to unlawful interception of wire and oral communications. *See* 18 U.S.C. §§ 2518(10)(a) & (c). An "aggrieved party" still has, however, constitutional remedies, if any apply. 18 U.S.C. § 2518(10)(c).
[36] *Id*.
[37] *Id.*

this complicated statutory scheme.[38] The most relevant section for the present discussion, 18 U.S.C. § 2703 (hereinafter "Section 2703") splits stored records into three categories: (1) communications stored less than 180 days; (2) communications stored more than 180 days; and (3) transactional/subscriber information.[39] Law enforcement agents can obtain communications stored less than 180 days solely with warrant,[40] whereas it can obtain stored communications more than 180 days old with a warrant, or on a showing of "specific and articulable facts [that the communications sought] are relevant and material to an ongoing criminal investigation," or an administrative subpoena requiring notice to the subscriber.[41] Finally, and most importantly for the present discussion, law enforcement agents may obtain transactional records with either a warrant or a showing that there are "specific and articulable facts showing that [the records sought] are relevant and material to an ongoing criminal investigation."[42]

2. PEN REGISTER PROVISIONS

[19] The Pen Register Provisions regulate how and when law enforcement may install pen registers and trap and trace devices.[43] A pen register is a device (now usually a piece of software) that "records or decodes dialing, routing, addressing, or signaling information (DRAS) transmitted by an instrument or facility from which a wire or electronic communication is

[38] For a lengthy explanation of the intricacies of the SCA *see* Orin S. Kerr, Symposium, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (classifying the SCA's treatment of content/non-content records differently than I have); *see also* Deidre K. Mulligan, Symposium, *Reasonable Expectations in Electronic Communications: A Critical Perspective of the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004).
[39] 18 U.S.C. § 2703 (2006).
[40] *Id*. § 2703(a).
[41] *Id*. §§ 2703(b) & (d).
[42] *Id* .§§ 2703(c) & (d). Subscriber records, a very narrow class of records defined in the statute, are obtainable through an administrative subpoena. *Id*.
[43] 18 U.S.C. § 3121-3127. Courts and commentators often use the term "pen register" to refer to both pen registers and trap and trace devices, probably because the "device" is usually the same piece of software. Thus all references to "pen register" hereafter refer to the combination of a pen register and a trap and trace device, unless otherwise noted.

transmitted."[44] A trap and trace device provides essentially the same data as a pen register - except that it records incoming DRAS information.[45] By definition, DRAS information excludes the contents of electronic or wire communications.[46]

[20] A court receiving an application for a pen register from a law enforcement officer or a U.S. Attorney must grant the application so long as it is complete.[47] The only substantive element of the application requires that the applicant must certify that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[48] Law enforcement officers have no obligation ever to disclose the existence of a pen register,[49] and even if they were to do so, aggrieved parties have no statutory suppression remedy, as they have for defective wiretap applications.[50]

3. TRACKING DEVICE STATUTE

[21] One final statutory provision worth mentioning because of later courts' reliance upon its language is 18 U.S.C. § 3117 (hereafter the

[44] *Id*. § 3127(3). Prior to the passage of the Patriot Act, pen registers were much more limited in their scope. The prior version of the statute defined a pen register 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…" 18 U.S.C. § 3127(3) (1988) (amended 2001).
[45] *Id*. § 3127(4).
[46] *Id*. § 3127(3).
[47] *Id*. § 3123(a) *See also* Susan Freiwald, Uncertain Privacy: Communication Attributes After the Digital Telephony Act, 69 S. CAL. L. REV. 949, 972 note 113 (1996) (examining the treatment of communications attributes in electronic surveillance law before and after CALEA, the debate over the scope and treatment of "call setup" information, and foreshadowing the present issue over law enforcement acquisition of prospective cell site data).
[48] 115 Stat. 278, 288-89.
[49] In fact, the Pen Register Provisions explicitly forbid service providers who receive pen register orders from disclosing the existence of such an order to the target. *See* 18 U.S.C. § 3123(d). In the author's own experience, however, the existence and records of a pen register are usually disclosed in discovery if the investigation results in a criminal indictment since the government will often use the pen register evidence at trial.
[50] *See* 18 U.S.C. § 2518(10)(a) (2006). Under current Fourth Amendment case law, an aggrieved party doesn't have a constitutional suppression remedy either. *See* discussion of *Smith v. Maryland* in Section III(B)(3), *infra*.

"Tracking Device Statute").[51] The Tracking Device Statute empowers a court, which is otherwise authorized to issue warrants, to issue a warrant for the installation and use of a tracking device within its own jurisdiction, as well as use of the device outside of its jurisdiction.[52] The legislative history of this statute shows that it was meant only to clarify jurisdictional issues relating to the authorization of a tracking device and "does not affect current legal standards for the issuance of such [a tracking device] order."[53] As shown below in Section V(B)(4), caselaw and an amendment to the Federal Rules of Criminal Procedure have abrogated any particular relevance this statute may have had.

C. FOURTH AMENDMENT

[22] As described above, the Supreme Court in *Katz* held that "the Fourth Amendment protects people and not places."[54] A line of cases followed that interpreted the *Katz* reasonableness standard in light of the government's use of sensory enhancement equipment, including "beepers" and other tracking devices.[55]

[23] In *United States v. Knotts*, the Supreme Court held that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[56] Because the "beeper" revealed no more information than standard visual surveillance, the search did not implicate the Fourth Amendment.[57] The following year in *United States v. Karo*, the Supreme Court revisited the practice of law enforcement use of beepers, but this time the beeper entered into a private residence.[58] The *Karo* court recognized the sanctity

[51] 18 U.S.C. § 3117(a) (2006).
[52] *Id*.
[53] S. Rep. No. 99-541, at 34 (1986).
[54] Katz v. United States, 389 U.S. 347, 351 (1967).
[55] For more on the use of "beepers" and other tracking devices, see generally Timothy Joseph Duva, Comment, *You Get What You Pay For…And So Does the Government: How Law Enforcement Can Use Your Personal Property to Track Your Movements*, 6 N.C.J.L & TECH. 165 (2004); Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo, and the Questions Still Unanswered*, 34 CATH. U.L. REV. 277 (1985).
[56] United States v. Knotts, 460 U.S. 276, 281 (1983).
[57] *Id.* at 282.
[58] United States v. Karo, 468 U.S. 705 (1984).

of a person's residence and reiterated that "[s]earches and seizures inside a home without a warrant are presumptively unreasonable…."[59] The court ultimately held that "[warrantless] monitoring of a beeper in a private residence . . . violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."[60]

[24] More recently, the Supreme Court refined its position on the use of sensory enhancement in *United States v. Kyllo.*[61] The law enforcement agents in *Kyllo* had used a heat-sensing imager to get a "crude visual image of the heat radiated from outside the house" which the agents then used, with other information, to procure a search warrant for the house.[62] The Court began its analysis by reiterating the sanctity of the home in Fourth Amendment analysis: "'[a]t the very core' of the Fourth Amendment 'stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[63] The five member majority held 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."[64] The Court recognized that while the actual technology law enforcement agents used in that case was not particularly accurate and did not reveal much information about what was happening inside of the home, a warrant would protect citizens from more intrusive technology "already in use or in development."[65]

[25] In 2003, the Sixth Circuit addressed whether the government's warrantless acquisition of cell site tracking data violated the Fourth

[59] *Id.* at 714-15.
[60] *Id*. at 714.
[61] Kyllo v. United States, 533 U.S. 27 (2001).
[62] *Id.* at 30. For more on the technology used by law enforcement in this case and other related technologies, see Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 540-44 (2005).
[63] *Kyllo*, 533 U.S. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).
[64] *Id.* at 34 (citation omitted). *Kyllo* was a close case with an unusual five member majority: Justice Scalia wrote the opinion and Justices Souter, Thomas, Ginsburg and Breyer joined him.
[65] *Id*. at 35-36.

Amendment rights of the cellular phone owner.[66] The law enforcement agents in *United States v. Forest* had successfully petitioned for a Title III Wiretap order to obtain communications from defendant Garner's phone.[67] The order also required the service provider to disclose "all subscriber information, toll records and other information relevant to the government's investigation."[68]

[26] While visually tracking the defendants driving in their car, the agents lost sight of the defendants.[69] An agent then called Garner's cellular phone several times, but did not let it ring, in order to obtain cell site data from the cellular provider.[70] The agents used the cell site data to regain visual contact with the defendants and they arrested the defendants on drug charges the following day.[71]

[27] The defendants in *Forest* challenged the acquisition and use of the cell site data under both the Wiretap Act and the Fourth Amendment. It is unclear on exactly what grounds under the Wiretap Act the defendants attacked the use of the cell site data since they did not challenge the validity of the court-approved wiretap order in place. Nonetheless, the court held that the cell site data the agents acquired was not a "communication" under the Wiretap Act, and even if it were a communication, the defendants had no suppression remedy because the "communication" was best characterized as an electronic communication.[72] In addressing the defendants' claim that the cell site data turned the cellular phone into a "tracking device" under the Tracking Device Statute, the court held that the Tracking Device Statute provided no statutory suppression remedy because it does not prohibit the use or

[66] United States v. Forest, 355 F.3d 942 (2003), cert. denied, 125 S.Ct. 174 (2004), reversed on other grounds, 543 U.S. 1100 (2005).
[67] *Id*. at 947.
[68] *Id*.
[69] *Id.*
[70] *Id.* at 948. The call to the defendant's cell phone presumably generated a single cell site data record.
[71] *Id.*
[72] *Id.* at 949. As stated in note 28, *supra*, the Wiretap Act excludes from the statutory suppression remedy all "electronic communications." *See* 18 U.S.C. §§ 2518(10)(a) & (c) (2006).

installation of a tracking device with or without a warrant or through another statutory means.[73]

[28] Turning to the Fourth Amendment, the court found the facts comparable to *Knotts*, and implicitly distinguishable from *Karo*, in that the agents tracked the cell site data only while the defendant was traveling on public highways.[74] While the court recognized that Garner may have had a reasonable expectation of privacy in his cell-site data, the court nonetheless rejected his claim because the agents had obtained no more information than they could have by mere visual surveillance.[75]

[29] Finally, several courts have relied on the Supreme Court's decision in *Smith v. Maryland*, which held that acquisition of prospective cell site data does not implicate the Fourth Amendment.[76] Several years prior to the enactment of the ECPA, the Court examined the constitutionality of law enforcement's warrantless use of a pen register.[77] The police installed a pen register device on the defendant's telephone, with the help of the phone company[78] to capture the numbers dialed. The Court first clarified that the police had not intruded into a constitutionally-protected space or invaded the defendant's property, but rather that the facts were more analogous to *Katz*. Following the *Katz* test, the Court held that the defendant could not have had either a subjective or an objectively reasonable expectation of privacy in the telephone numbers he dialed because such numbers were voluntarily conveyed to a third party. According to the Court, the defendant should have known that the phone company could record the numbers.[79]

---

[73] *Forest*, 355 F.3d at 950 (adopting the reasoning and holding of United States v. Gbemisola, 225 F.3d 753, 758 (D.C.Cir. 2000), *cert. denied*, 531 U.S. 1026 (2000)).
[74] *Id*. at 951-52.
[75] *Id*. at 951.
[76] Smith v. Maryland, 442 U.S. 735 (1979).
[77] *Id.* at 736.
[78] The Court defined the pen register device as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released." *Id.* at 736 n. 1 (quoting United States v. New York Tel. Co., 434 U.S. 159, 161 n.1 (1977)).
[79] *Id*. at 745.

IV. RECENT CASES ADDRESSING THE ACQUISITION OF CELL SITE DATA

A. INTRODUCTION

[30] Prior to August 25, 2005, no court in the United States had established the standard the government must meet to obtain a court order allowing prospective acquisition of cell site tracking data. Magistrate Judge James Orenstein issued the first decision on the issue in *E.D.N.Y. Decision I*,[80] when he found that, while the government may obtain *historical* cell site data based on the specific and articulable facts standard of the Stored Communications Act, it may procure *prospective* cell site data only after making a showing of probable cause.[81] Shortly after this decision, Magistrate Judge Stephen Wm. Smith issued an extensive opinion, fully analyzing the issue and coming to the same conclusion as Magistrate Orenstein.[82] Magistrate Orenstein, on reconsideration, issued a lengthier opinion several weeks later, relying in part on Magistrate Smith's intervening decision.[83] Because Magistrate Smith's analysis in the *Texas Decision* forms the analytical basis for over a dozen subsequent cases in a short period, I describe that decision before noting where other cases have agreed, disagreed, or otherwise diverged.

B. THE TEXAS DECISION

[31] In the *Texas Decision*, the government applied for, among other things, (1) a pen register order; and (2) an order for subscriber records including

> the location of cell site/sector (physical address) at call origination (outbound calling), call termination (for incoming calls), and, if reasonably available, during the progress of a call." [] Also sought [was] information regarding the strength, angle, and timing of the caller's signal measured at

[80] E.D.N.Y. I, 384 F. Supp. 2d 562 (E.D.N.Y. 2005).
[81] *Id.* at 564.
[82] Texas Decision, 396 F.Supp.2d 747 (S.D. Tex. 2005).
[83] E.D.N.Y. Decision II, 396 F.Supp. 2d 294 (E.D.N.Y. 2005).

> 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.[84]

[32] In setting the stage for its subsequent analysis, the court described the statutory scheme and related procedural standards as follows:

- 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).[85]

[33] The court began its analysis with the Tracking Device Statute, finding that it "appears at first glance to provide the most likely fit for cell site [data]."[86] The court examined the statutory language and legislative history of the Tracking Device Statute and found that Congress had drafted the definition of "tracking device" broadly enough to cover the use of cell site data to track individuals.[87] The government had argued that the use of prospective cell site data did not turn a cell phone into a "tracking device" because (1) the legislative history of the Tracking Device Statute showed the definition merely referred to "one-way radio 'homing devices;'"[88] and (2) prospective cell site data does not provide detailed and precise location information.[89] The court rejected this argument and found that Congress, by using a broader definition of the term "tracking device" under the Tracking Device Statute than that used in the legislative history's glossary definition, meant to afford the term a broader meaning.[90] According to the court, the precision or accuracy of

[84] *Texas Decision*, 396 F. Supp. 2d at 749.
[85] *Id.* at 753.
[86] *Id.* at 753.
[87] *Id.* at 754-55.
[88] *Id.* at 753 (quoting S. Rep. No. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564).
[89] *Id.* at 755.
[90] *Id.* at 754.

cell site data was immaterial because "§ 3117(b) does not distinguish between general vicinity tracking and detailed location tracking."[91] Moreover, even if there were such a distinction in the statute, the court found that present technology does, or at least has the potential to, provide detailed and precise location information.[92]

[34] The court then addressed the Fourth Amendment issues implicated by cell site data. The court distinguished *Smith v. Maryland* on the grounds that, unlike dialed telephone numbers, "cell site data is not 'voluntarily conveyed' by the user to the phone company [but rather is sent] automatically . . . entirely independent of the user's input, control, or knowledge."[93] The court found support for the proposition that the cellular phone owner retained a reasonable expectation of privacy in his cell site data from a portion of the Wireless E-911 legislation.[94] The statute provides that a consumer "shall not be considered to have approved the use or disclosure of or access to . . . [cellular] call location information," except in an emergency situation or with the consumer's prior consent.[95] In dicta, the court acknowledged that some monitoring of cell site data may be permissible under the Fourth Amendment (*i.e.* when the user is traveling on public highways) but urged prosecutors nonetheless to obtain Rule 41 warrants to avoid any potential Fourth Amendment violations.[96] Ultimately, the court held that "prospective cell

[91] *Id.* at 755.
[92] *Id.* at 755. The court further noted that the Department of Justice's own manuals describe the common usage of tracking devices which use cellular towers and GPS, noting their precision. *Id*. at 755.
[93] *Id.* at 756.
[94] *See id.* at 757.
[95] *Id.* at 757 (quoting from 47 U.S.C. § 222(f)). It would not be hard to imagine, however, that cellular services contracts may currently or in the future provide that the consumer expressly consents to disclosure of cell site data to third parties (e.g. for the purposes of location-based advertising). Such a contract clause would seem to suggest that a user has no reasonable expectation of privacy in such information, and thus no Fourth Amendment protection. On cellular location based advertising already in use, see Communicate Magazine, *Big names deploy location-based marketing - location-based marketing via cellular phone*, September 2001, *available at* http://www.findarticles.com/p/articles/mi_m0BKU/is_2001_Sept/ai_79125278 (last visited May 13, 2006). *Cf. Freedman v. American Online, Inc.*, 412 F. Supp. 2d 174, 182-183 (D.Conn. 2005).
[96] *Texas Decision*, 396 F. Supp. 2d at 757.

site data is properly categorized as tracking device information under [the Tracking Device Statute]."[97]

[35] The court next examined the Pen Register Provisions. The court found that Congress, through the Communications Assistance for Law Enforcement Act (CALEA), had made its intent clear that pen registers, by themselves, could not be used to acquire location information.[98] The pertinent section of CALEA provides that:

> [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).[99]

[36] The court dismissed the possibility that the "Super Warrant"[100] protections of the Wiretap Act apply to cell site data because such data does not constitute the contents of a communication.[101] It similarly rejected the first two sections of the SCA on the basis that they also protected the contents of a communication.[102] With regard to 18 U.S.C. § 2703(c), which regulates access to transactional records, the court found that prospective cell site data did not fit the definition of "record[s] pertaining to 'wire or electronic communications'" because the definition of "electronic communications" expressly excludes communications from

---

[97] *Id.*
[98] *Id*. at 757-58 (quoting 47 U.S.C. § 1002(a)(2) (2006)). For a discussion of the changes made by CALEA to the existing statutory scheme see Freiwald, *supra* note 47.
[99] 47 U.S.C. § 1002(a)(2)(B) (2006).
[100] The term "Super Warrant" was coined by Orin S. Kerr. *See* Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT ACT: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 645 (2003).
[101] *Texas Decision*, 396 F. Supp. 2d at 758.
[102] *Id.* (citing 18 U.S.C. § 2703(a)&(b) (2006); 18 U.S.C. § 2711(1) (2006)) (incorporating into the SCA the definition of "contents" from the Wiretap Act, 18 U.S.C. § 2510(8)).

a tracking device.[103] The court also reasoned that the structure of the ECPA shows that the SCA was meant to apply only to *existing* records and not *prospective* records.[104] The court came to this conclusion because, unlike the Wiretap and Pen Register Statute sections of the ECPA which provide precise time limits for use and renewal as well as for temporary sealing of orders, the SCA lacks time limits and does not require sealing of the order, presumably because revealing the existence of an SCA order would not disrupt ongoing surveillance.[105]

[37] In support of its application, the government contended that the authority of a pen register order, combined with the authority of an SCA order, sufficed to authorize law enforcement to obtain prospective cell site data. The government argued that cell site data is DRAS[106] (specifically "routing" data) under the Pen Register Provisions. It argued that, while under the restriction added by CALEA the government cannot obtain cell site data *solely* by using the Pen Register Provisions, it can nonetheless obtain such data if it combines the authority of the Pen Register Provisions with other authority.[107] According to the government, this additional authority can be found in the SCA.[108] Essentially this "hybrid theory" takes the prospective and DRAS features of the Pen Register Provisions and combines them with the legal standard and transactional records features of the SCA.

[38] The court rejected the government's hybrid theory argument on several grounds. First, it explained that the legislative history of the PATRIOT Act[109] clarified that DRAS was meant merely to allow pen registers to obtain internet traffic data.[110] Moreover, even if DRAS included more than just internet traffic data, the court reasoned that DRAS information must be "generated by, and incidental to, the transmission of

[103] *Id.* at 758-59 (quoting 18 U.S.C. § 2510(12)(C)).
[104] *Id.* at 760 (emphasis added).
[105] *Id*.
[106] *See* note 41 *supra* and accompanying text..
[107] *Texas Decision*, 396 F. Supp. 2d at 761.
[108] *Id*.
[109] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2006).
[110] *Texas Decision*, 396 F. Supp. 2d at 761-62.

'a wire or electronic communication.'"[111] Since a user generates cell site data whether or not engaging in a wire or electronic communication, the court found that it was not included in the definition of DRAS.[112]

[39] Again looking at legislative history, the court also found that Congress did not intend Section 1002 to change electronic surveillance law, but rather to clarify and reiterate the existing electronic surveillance regime regarding location data.[113] It examined the statements of then-FBI Director Louis Freeh, who had testified at length in response to worries by privacy advocates that CALEA's amendments would allow law enforcement to obtain cell phone tracking data via the Pen Register Provisions. Specifically, Freeh testified that CALEA was not meant to "enlarge or reduce the government's authority [regarding electronic surveillance],"[114] that "'transactional information' is . . . exclusively dealt with in [the SCA]," and that CALEA did not relate to or affect the SCA.[115] Freeh's disclaimer that law enforcement could not obtain location information through the use of a Pen Register was eventually codified as Section 1002. Based on these statements, and the lack of cross-referencing between the SCA and the Pen Register Provisions, the court held that Congress could not have meant the SCA to be the additional authority required under Section 1002 to obtain location data and thus rejected the "hybrid theory" application.[116] The court concluded by noting that, should the government wish, it could surely apply for a Rule 41 warrant in order to obtain the cell site data it sought.[117]

---

[111] *Id.* at 762 (citing 18 U.S.C. §3127(3) (2004)).
[112] *Id.*
[113] *Id.* at 765-66 (citing Freiwald, *supra* note 47).
[114] *Id.* at 763 (quoting *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) (1994) [hereafter Freeh Statement]; *see also* Freiwald, *supra* note 47, at 976-82.
[115] *Texas Decision*, 396 F.Supp.2d at 764. *See also* Freiwald, *supra* note 47, at 976-982 (citing Freeh Statement, *supra at* 27-28.)
[116] *Id.* at 764-65.
[117] *Id. at* 765. As noted below, several courts have denied an application for an order under the "hybrid theory" and then later granted the same order upon a showing of probable cause under Rule 41.

C. CASES FOLLOWING THE TEXAS DECISION

[40] To date, more than a dozen decisions have come down either denying or granting the acquisition of real-time and/or prospective cell site data. At least seven of those decisions have generally adopted the reasoning of the Texas Decision, rejected the government's "hybrid theory," and denied the applications.[118] Several of these decisions add additional important analysis and note small disagreements with the Texas Decision, which are discussed below.

[41] The first court to rule on the issue following the E.D.N.Y. and Texas Decisions simply held that it was adopting the reasoning of those decisions and that the court and two fellow Magistrate Judges would not approve applications for prospective cell site data predicated upon the authority of the SCA, the Pen Register Provisions, or a combination of the two.[119]

---

[118] *In re* Applications of the United States of America 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.C. Cir. Oct. 26, 2005) [hereinafter D.C. Decision I]; *In re* Application Of The United States Of America For An Order Authorizing The Installation & Use Of A Pen Register & A Caller Identification System On Telephone Numbers [Sealed] & [Sealed] & The Production Of Real Time Cell Site Information, 402 F. Supp. 2d 597 (D. Md. 2005) [hereinafter Maryland Decision I]; *In re* Application Of The United States Of America For An Order Authorizing The Release Of Prospective Cell Site Information, 407 F. Supp. 2d 132 (D.C. Cir. 2005) [hereinafter D.C. Decision II]; *In re* Application Of The United States Of America For An Order Authorizing The Release Of Prospective Cell Site Information, 407 F. Supp. 2d 134 (D.C. Cir. 2006) (Facciola, M.J.) [hereinafter D.C. Decision III]; Wisconsin Decision, 412 F. Supp. 2d 947 (E.D. Wis. 2006); *In re* Application Of The United States Of America For An Order Authorizing The Installation & Use Of A Pen Register &/Or Trap & Trace For Mobile Identification Number (585) 111-1111 & The Disclosure Of Subscriber & Activity Information Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) [hereinafter W.D.N.Y. Decision]; *In re* Application Of The United States Of America For Orders Authorizing The Installation & Use Of Pen Registers & Caller Identification Devices On Telephone Numbers [Sealed] & [Sealed], 416 F. Supp. 2d 390 (D. Md. 2006) [hereinafter Maryland Decision II]; *In re* Application Of The United States 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 S.D.N.Y. II].

[119] *D.C. Decision I*, Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531. Magistrates Kay and Facciola joined in the decision. Magistrate Facciola has since weighed in twice on the issue. *See D.C. Decision II,* 407 F. Supp. 2d 132; *D.C. Decision III*, 407 F. Supp. 2d 134.

[42] Magistrate Bredar soon clarified and narrowed the issues involved further when he elucidated the important distinction between "real-time" and "prospective" cell site data: Prospective cell site data consists of all data recorded by a cellular provider after the issuance of, and pursuant to, a court order, whereas real-time cell site data consists of "a subset of 'prospective' cell site information" that "refers to data used . . . to identity the location of a phone at the present moment."[120] Because the government had requested "real-time" cell site data, the court limited its holding to real-time cell site data, while suggesting that the analysis probably also applied to all prospective cell site data.[121]

[43] The Maryland court also discussed in dicta the Fourth Amendment issues implicated by the acquisition of prospective/real-time cell site data. The government had argued that it was never required to obtain a warrant when acquiring cell site data because under *Smith v. Maryland* cell site information is "voluntarily" conveyed to a third party.[122] The court briefly suggested that cell site data could be distinguished from numbers dialed since the cell phone automatically transmits such information, regardless of whether the user dials a phone and because most users likely aren't aware they are transmitting their location.[123] The issue of the reasonable expectation of privacy in prospective cell site information is discussed further in Section V(B).

[44] As the court recognized, however, since the government had asked for an *order*, it must have some statutory basis for granting that order. Since the SCA and the Pen Register Provisions do not provide that authority, the court concluded that when the government seeks an order authorizing the acquisition of real-time cell site data in the future it must present an affidavit showing probable cause per Rule 41.[124] The court

[120] *Maryland Decision I*, 402 F. Supp. 2d at 599. The court provides an excellent example that shows the difference between the two concepts in footnote 5.
[121] *Id.* at 605 n. 11. Indeed, in a follow-up decision, Magistrate Bredar held that the reasoning of his initial decision on real-time cell site data applied equally to prospective cell site data. *Maryland Decision II*, 416 F. Supp. 2d at 395.
[122] *Maryland Decision I*, 402 F. Supp. 2d at 605 n. 12.
[123] *Id.* (noting "I do not believe most cell phone possessors realize they can be located within 100-300 meters any time their phone is turned on."). *See also* Texas Decision, 396 F.Supp.2d 747, 751 (S.D. Tex. 2005).
[124] *Maryland Decision I,* 402 F. Supp. 2d at 605.

noted that, immediately following its denial of the present application, the government presented an affidavit establishing probable cause under Rule 41 and the court issued the requested order.[125]

[45] Soon thereafter, the government tried a creative new approach, when it requested prospective cell site data by making a showing of "*probable cause* to believe that the requested prospective cell site information is *relevant and material* to an ongoing criminal investigation."[126] The D.C. court found this "meld[ing]" of the Pen Register Provisions standard with the constitutional probable cause standard to be amusing, but nonetheless inadequate.[127] The court ultimately found that the "probable cause" language added nothing to the Pen Register Provisions application and that the showing did not meet the constitutional "probable cause" standard.[128]

[46] Less than a month later, the government again sought an order for cell site data from the same magistrate judge, but this time it "set[] forth facts demonstrating *probable cause* to believe that the requested cell site information is *relevant and material* to an ongoing criminal investigation" and submitted an affidavit regarding such facts by an investigating agent.[129] The court found that, yet again, the government had missed the constitutional standard for probable cause: The showing is probable cause

[125] *Id.* at 598 n. 1.

[126] D.C. Decision II, 407 F. Supp. 2d 132,132-33 (D.C. Cir. 2005) (emphasis added). The U.S. Attorney's Office is a very well organized organization. I assume for the purposes of this paper that all regional offices act in a concerted manner and that this new approach was not the result of a "rogue" office, but rather a shift in strategy directed by the main office.

[127] *Id.* at 133 ("I am afraid that I find the government's chimerical approach unavailing. Indeed, and to keep the animal metaphor going, it reminds one of the wag who said a camel is a horse planned by a committee.")

[128] *Id*. While the decision does not discuss Section 1002, it seems that the government, recognizing that it could not obtain cell site data "solely" through the Pen Register Statute, may have believed that by adding the words "probable cause to believe" it had invoked the Rule 41 standard and therefore added the additional authority Section 1002 required to obtain cell site data.

[129] D.C. Decision III, 407 F. Supp. 2d 134, 135 (D.C. Cir. 2006) (emphasis added). This is one of just three cell site decisions where the court states (albeit in very general terms) the factual basis underlying the application. Briefly, the affidavit of the investigating agent described an investigation of a suspected drug dealer and asserted that the government sought cell site information to determine the location of the suspect's stash in another state.

to believe that the information sought *is itself evidence of a crime*, not that it is relevant and material to an ongoing investigation.[130]

D. CASES REJECTING THE E.D.N.Y. AND TEXAS DECISIONS

[47] Not all courts that have encountered this issue have agreed with the Texas Decision's analysis – two courts have accepted the government's "hybrid theory" while a third granted the government's application on other grounds.[131] In *S.D.N.Y. I*, the court first distinguished the facts before it from those of the then-existing decisions on three grounds: (1) Whereas in the prior cases, the government had asked for cell site information *during* calls and perhaps even when no call was being made or received, here the government's application asked only for cell site data at the beginning and end of each call; (2) whereas in the prior cases, the government had asked for triangulation data, here the government asked only for data from a single cell tower at a time (*i.e.* single cell site data); and (3) whereas in the prior cases the government had obtained the information directly, here the cellular provider would be required to give raw data to the government, which would translate the data into a spreadsheet.[132] The court found these distinctions important because it meant the government could obtain only general location data and only when that user dialed the phone (*i.e.* "voluntarily transmitted" the cell site data).[133]

[48] The court examined the Pen Register Provisions and found that the statute "would by itself provide authority for the order sought by the Government were it not for [Section 1002]."[134] The court reasoned that the legislative history of Section 1002 shows that Congress understood

---

[130] *Id.*; FED. R. CRIM. P. 41.

[131] S.D.N.Y. I, 405 F. Supp. 2d 435 (S.D.N.Y. 2005); Louisiana Decision, 411 F.Supp.2d 678 (W.D. La. 2006); *In re* Application Of The United States Of America For An Order Authorizing The Installation & Use Of A Pen Register With Caller Identification Device & Cell Site Location Authority On A Certain Cellular Telephone, 415 F. Supp. 2d 663, 666 (S.D. W.Va. 2006) (Stanley, M.J.) [hereinafter West Virginia Decision]. The West Virginia Decision is addressed separately in the next section.

[132] *S.D.N.Y. I*, 405 F. Supp. 2d at 437-38. It is far from clear that the means by which the government would obtain cell site data under the application in this case is any different from how it would have obtained cell site data in any of the other reported decisions.

[133] *Id.* at 449-50.

[134] *Id.* at 440.

that prospective cellular location data could, prior to the passage of Section 1002, be obtained under the Pen Register Provisions.[135] Working backwards, the court first found that a pen register is the *only physical device* that could obtain prospective cell site data and therefore if Section 1002 were meant to remove the government's ability to obtain cell site data through using a pen register, whether combined with other authority or not, the government would have no means of obtaining prospective cell site data.[136] Because it believed that Congress could not have meant to take away the government's ability to obtain prospective cell site data, the court held that the term "solely pursuant" means that the government can obtain prospective cell site data "through some unexplained combination of the Pen Register Provisions with some other unspecified mechanism."[137]

[49] The court next turned to the SCA and determined that, under the plain language of the statute, cell site data is "'information' . . . in the form of a 'record'" because it is first created by the cellular provider and then sent to the government.[138] The court rejected the theory that the "service" being provided by the cellular provider was that of a "tracking device" and instead held that the "service" was cellular voice and data services.[139] Finally, the court explained that, at least under the specific facts of the present case, the SCA could be used to obtain prospective cell site data because the service provider was storing the data before handing it to the government. The court reasoned that even under a very narrow reading of the SCA, "the Government [could] present[] daily or hourly (or even more frequent) applications to the Court to obtain historical cell site data."[140]

---

[135] *Id.* at 440-41.

[136] *Id*. at 441-42. 18 U.S.C. § 3121 provides that government cannot install a pen register except under the authority of the Pen Register Statute (and, though not relevant here, FISA).

[137] *S.D.N.Y. I*, 405 F. Supp. 2d at 442-43. While it accepted the proposition that the Pen Register Provisions must be combined with some other "unspecified mechanism" to obtain prospective cell site data, the court seemed uncomfortable with this statutory interpretation, calling it "unsatisfying[]" and "unattractive", but nonetheless adopted it because the alternative interpretations would lead to absurd results.

[138] *Id.* at 447.

[139] *Id.* at 444-45.

[140] *Id.* at 447. This reveals an inherent problem with applying traditional principles of surveillance to electronic communications and related transactional information: The difference between *intercepting* an electronic communication or related transactional

Further, the court reasoned if one accepts that the Pen Register Provisions are a necessary component for obtaining prospective cell site data, then the SCA is the perfect statute to combine with the Pen Register Provisions because together they allow the acquisition of "records" by a pen register device using the higher legal standard of the SCA with the time limit protections of the Pen Register Provisions.[141]

[50] The court rejected any Fourth Amendment constitutional protection as applied in this case for several reasons. First, the court reasoned information provided "in this District" consisted of only very general location data, as opposed to "pinpoint" data.[142] The court distinguished *Karo* because the cell site data was not accurate enough to disclose the user's location *within* a home and because, unlike *Karo*, "the Government does not seek to install [a] 'tracking device:' The individual has chosen to carry a device and to permit transmission of its information to a third party…."[143]

[51] The court ultimately accepted the "hybrid theory," at least as applied to the particular application the government presented. Realizing that technology could and probably would change in the near future, the court limited its holding by restricting what information it would grant in the future under a "hybrid theory" application. The court stated that in the future it would sign only orders that required the production of:

> (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

information and *obtaining stored* versions of the same electronic communication or related transactional information is almost nonexistent. I discuss this issue in further detail in Section V(B)(3).

[141] *Id*. at 448. The court agreed that the SCA is "unsuited" for an order authorizing ongoing acquisition of cell site data because of its lack of time limitations and its retrospective nature but found that when combined with the Pen Register Statute, the SCA adopts the time limitations and prospective aspects of that statute. *Id*. at 447-48.

[142] *Id*. at 449.

[143] *Id*. The court cited *Smith v. Maryland* for this proposition, but did not reach the question of whether cell site data is "voluntarily conveyed" when the user is not making or receiving a call, since the government in this case requested only cell site data at the beginning and end of calls. *Id*. at 449-50.

> 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.[144]

[52] The court concluded that, should the government wish to obtain any other or more exact cell site data, such as triangulation cell site data or cell site data during a call, it would need to "provide additional briefing on why such information is permissible under the relevant authorities."[145]

[53] One court has since followed and adopted the reasoning of this case.[146] A Louisiana court also briefly examined the issue of GPS technology, finding that several cell phone companies, including Nextel, have cell phones that use GPS technology.[147] However, since the government was not requesting GPS data, the court did not reach the issue of whether such information could be obtained through a "hybrid theory" application. The court specifically limited its holding and expressly stated that the government was not allowed to obtain following information:

> (1) any cell site information that might be available when the user's cell phone was turned "on" but a call was *not* in progress; (2) information that would allow the Government to triangulate multiple tower locations and thereby pinpoint the location

[144] *Id. at* 550. I do not find the court's limiting language particularly helpful. There is no practical difference between obtaining cell site data from a single cell site at the time a call is placed/received and obtaining cell site data from multiple cell sites during a call. For instance, law enforcement agents could create a software program that dialed the user's cell phone every ten seconds and then hang up before the cell phone user actually heard a ring (the practice of "pinging" a phone.) Each call would create a single cell site record which, in the aggregate, would provide the same cell site data as a pen register that recorded cell site data continuously. *See, e.g., Forest, supra* note 66, at 947 (police "pinged" defendant's phone several times, hanging up before the defendant's phone rang).

[145] *S.D.N.Y. I*, 405 F. Supp. 2d at 480.

[146] Louisiana Decision, 411 F.Supp.2d 678 (W.D. La. 2006).

[147] *Id.* at 681.

> of the user; and (3) GPS information on the location of the user, even if that technology is built into the user's cell phone.[148]

E. VARIATION ON THE THEME

[54] One court has approved an application for prospective cell site data on completely different grounds than all others. In the *West Virginia Decision*, the court held that, because the current possessor of the cell phone was not the *subscriber*, the Pen Register Provisions by themselves provided the required authority to obtain prospective cell site data.[149] The current possessor of the cell phone was a fugitive who was neither the subscriber nor the owner of the phone.[150] The court rejected the "hybrid theory" but granted the application because it found that, under the plain language of the statute, the exception in Section 1002 applies only to "*the physical location of the subscriber*."[151] Since the current "user" was not a "subscriber," the court held that the exception in Section 1002 did not apply and therefore the Pen Register Provisions, by itself, provided the requisite authority to obtain cell site information.[152]

F. SUMMARY

[55] The courts have split on whether a "hybrid theory" application (*i.e.* an application for an order under the combined authority of the Pen Register Provisions and the SCA) is sufficient to allow the government to obtain prospective and/or real-time cell site data. The majority of courts that have addressed the issue have held, based upon the legislative history, the structure of the statutory scheme, and Fourth Amendment jurisprudence, that a "hybrid theory" application does not present the requisite authority for the government to obtain prospective cell site data. Two courts have dissented, approving "hybrid theory" applications on the narrow

[148] *Id.* at 683.
[149] West Virginia Decision, 415 F. Supp. 2d 663, 666 (S.D. W.Va. 2006).
[150] *Id.* at 664. It is unclear whether the fugitive had stolen the cellular phone or simply borrowed a friend's cellular phone.
[151] *Id.* at 665 (emphasis added).
[152] *Id.* at 665-66. This case did not really approve of the "hybrid theory" (indeed, it rejected the theory) but approved the application solely upon the authority of the Pen Register Statute under the narrow facts of the case.

applications before them, on the grounds that the Pen Register Provisions are a required component of any application for prospective cell site data, and that the SCA provides the additional authority required to obtain such data. A third court has approved an application for prospective cell site data on the narrow grounds that the statutory exception embodied in Section 1002 did not apply because the "user" of the cell phone was not the owner or subscriber of that cell phone, and thus, the Pen Register Provisions by itself provided the requisite authority to obtain prospective cell site data. To date, none of these decisions has been appealed, notwithstanding several courts' suggestion to the government to do so.[153]

V. WHAT STANDARD SHOULD A COURT APPLY?

A. INTRODUCTION

[56] At this time the government does not seem to be able to obtain cell site data (or any other cellular tracking data) directly using its own devices.[154] Since cellular providers are unlikely to voluntarily provide cell site data directly to government, the government must obtain an order directing the cellular providers' assistance in obtaining cell site data.[155]

---

[153] *See* S.D.N.Y. II*,* No. 06 CRIM. MISC. 01 2006 WL 468300, at *2 (S.D.N.Y. 2006); Texas Decision, 396 F.Supp.2d 747, 765 (S.D. Tex. 2005). It seems the U.S. Attorney's Office has made a conscious decision not to appeal any of these decisions. I believe the reason for this is that many magistrate judges are unfamiliar with the issue and still grant "hybrid theory" applications without written opinions, and the U.S. Attorney's Office is unwilling to risk negative higher court case law on this issue.

[154] If the government could do so, it would not need to apply for an order requiring cellular providers to provide help to the government in obtaining this information.

[155] While it seems one or more telecommunications providers have voluntarily provided some information to government agencies without a consumer's approval (*see, e.g.,* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006 at 1A), this author believes cellular providers are unlikely to give law enforcement prospective cell site data voluntarily for three reasons: (1) The enormous costs of complying with multiple requests from law enforcement agencies across the country; (2) the existence of privacy clauses in end-user cellular phone contracts (s*ee, e.g.,* T-Mobile Terms & Conditions, *available online at* http://www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true, at paragraph 16 (last visited May 9, 2007)); and (3) the possibility of strong consumer backlash if consumers were made aware of the cellular providers' actions.

[57] My analysis of which standard a court must apply in determining whether to grant an order authorizing the government to obtain prospective cell site data necessarily begins with dividing the issue into two parts: the statutory requirements to obtain an order (discussed in Section V(B)) and the constitutional restrictions, if any, on obtaining such data without a court order (discussed in Section V(C)). The statutory analysis assumes that, at least as to the acquisition of some cell site data, there are no constitutional restrictions. Section V(B) analyzes the statutory basis for obtaining an order requiring cellular providers to provide the government with prospective cell site data. In contrast, Section V(C) discusses constitutional restrictions, if any, on both the government's independent acquisition of cell site data and upon its acquisition of cell site data through cellular service providers.[156]

B. STATUTORY ANALYSIS

[58] As stated above in Section III(B), the statutory scheme setup by the ECPA (as amended) allows the government to obtain several types of electronic data: (1) the contents of electronic communications ("Wiretap Act");[157] (2) stored communications, subscriber and transactional records (SCA);[158] (3) dialing, routing, addressing, and signaling information ("Pen Register Provisions");[159] and (4) tracking device data ("Tracking Device Statute").[160] I consider whether each section provides the necessary authority to obtain prospective cell site data below.

1. WIRETAP ACT

[59] The Wiretap Act seems to be a poor candidate for obtaining cell site data. While the term "electronic communications" is defined very broadly

[156] There is no significant legal difference between the government obtaining cell site data directly or through the cellular provider. In the latter case, the cellular provider acts as an agent of the government for Fourth Amendment purposes. *See* Smith v. Maryland, 442 U.S. 735, 740, n. 4 (1979).
[157] 18 U.S.C. §§ 2511-2522 (2006).
[158] 18 U.S.C. §§ 2701-2712 (2006).
[159] 18 U.S.C. §§ 3121-3127 (2006).
[160] 18 U.S.C. § 3117 (2006).

under the Wiretap Act,[161] the Wiretap Act covers only the interception (i.e. real-time acquisition) of the "contents [of electronic communications]," a term which is defined as "any information concerning the substance, purport, or meaning of [a particular electronic] communication…."[162]

[60] Cellular telephones transmit an array of "communications" including voice communications, text messages, emails, instant messages, and other internet communications. The "contents" of these "communications" are spoken words (voice communications) and combinations of text and pictures (text messages, emails, instant messages, and other internet communications). All of these "contents" are expressions created directly by humans and communicated to/from another human (directly or indirectly).[163] Cell site data is an electronic communication in that it is a "transfer of . . . [a] signal . . . by a . . . radio" but it is not contents because it is automatically-generated data transmitted from a cellular handset – not a communication created directly by a human and communicated to another human.[164] I disagree with Magistrate Smith and several other courts' conclusion that, because the cell site data can be used to track an individual, that converts the cellular phone into a "tracking device" whose "communications" are exempted from the definition of "electronic communications."[165]

[61] Few, if any, cell phone users carry a cellular telephone for the purpose of sending tracking data to the cellular provider. Few, if any, cell phone users would consider their cell phone a "tracking device," at least

[161] "Electronic Communications" is defined 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--
(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds…" 18 U.S.C.S. § 2510(12) (2000 & Supp. 2006).
[162] 18 U.S.C. § 2510(8).
[163] *See*, Freiwald, *supra* note 47, at 957 (noting that "judges are used to thinking of communications as requiring two human parties," but noting the blurry line between contents and non-contents.)
[164] *Id.*; 18 U.S.C. § 2510(12) (2000 & Supp. 2006).
[165] *See, e.g.,* Texas Decision, 396 F.Supp.2d 747, 754 (S.D. Tex. 2005).

prior to learning about the cell site decisions discussed in this paper. The primary use of a cell phone is to send voice and data communications from person to person. Any cell site data sent from the cellular phone is merely data generated incidental to cellular communications and not communications themselves.[166]

[62] Moreover, the definition of "electronic communications" specifically excludes "communications from a tracking device," so even if it could be argued that cell site data turns a cellular phone into a "tracking device," law enforcement could not obtain the contents of a communication (i.e. the cell site data) from that tracking device through the Wiretap Act.[167]

[63] While the Electronic Frontier Foundation and other commentators have urged the courts to require a government agency seeking prospective cell site data to make the same showing and endure the same limitations imposed on the interception of electronic communications under the Wiretap Act,[168] the law does not seem to support the Wiretap Act provisions as a basis for obtaining cell site data.

2. PEN REGISTER PROVISIONS

[64] Prior to the passage of the Patriot Act in 2001 the terms "pen register" and "trap and trace device" were defined narrowly under the Pen Register Provisions.[169] Under the original ECPA version of the statute, a pen register was defined as:

> a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on

[166] *See, e.g.,* Freiwald, *supra* note 47, at 954 ("In general, communication attributes comprise information disclosing the event of the communication and fleshing out details of that event.").
[167] 18 U.S.C. § 2510(12) (2000 & Supp. 2006).
[168] *See* Brief for the Electronic Frontier Foundation as Amicus Curiae Supporting defendants, *In re* Application for Pen Register on Trap and Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747 (S.D. Tex. 2005); Memorandum from Susan Freiwald, Professor, University of San Francisco School of Law, to Author (2006) (on file with author) [hereinafter Freiwald Memo].
[169] *See* 18 U.S.C. §§ 2703(b) & (d) (2006).

> the telephone line to which such device is attached, but such term does not include any device 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 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[.][170]

[65] The first part of the definition (the text before "but") was changed by the Patriot Act to read "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."[171]

[66] This expanded definition, by itself, would seem to include cell site data since it is "routing [and] signaling information," information sent from the handset which assists the cellular provider in routing the communications to and from the handset and transmitting such signals.[172] Prior to the passage of the Patriot Act, however, Congress passed CALEA which added 47 U.S.C. § 1002(a)(2)(B).[173] As discussed earlier, Section 1002 provides that information disclosing the physical location of a subscriber (other than the phone number itself) cannot be obtained *solely* through the use of the Pen Register Provisions.[174] There is no indication in the legislative history of the Patriot Act that the amendment to Section

---

[170] 18 U.S.C. § 3127(3) (2006), *amended by* 18 U.S.C. § 3127(3), Pub.L. 107-56, Title II, § 216(c)(1) to (4), Oct. 26, 2001, 115 Stat. 290.
[171] 18 U.S.C. § 3127(3).
[172] *See, e.g.*, Maryland Decision II, 416 F. Supp. 2d 390, 394 (D. Md. 2006) (quoting United States Telecom Ass'n. v. F.C.C., 227 F.3d 450, 463-64 (D.C. Cir. 2000)) ("[A] mobile phone sends signals to the nearest cell site at the start and end of a call. These signals, which are necessary to achieve communications between the caller and the party he or she is calling, clearly are signaling information.") (citations omitted).
[173] 47 U.S.C. § 1002(a)(2)(B); *see generally* Freiwald, *supra* note 47.
[174] 47 U.S.C. § 1002(a)(2)(B) (emphasis added); Texas Decision, 396 F.Supp.2d 747, 757-58 (S.D. Tex. 2005).

3127(3) (adding DRAS to the definition of "pen register") was meant to overrule Section 1002.[175] Thus, while the Pen Register Provisions, as amended by the Patriot Act, seem by themselves to provide the authority for government acquisition of cell site data, that authority is explicitly limited by Section 1002.[176] Additionally, the pen register definition explicitly exempts from its scope:

> 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.[177]

[67] Cellular providers keep records of at least some cell site information by themselves for billing and "other like" business purposes, such as deciding where to build new cell sites or determining when to bill a user for "roaming" charges.[178] If cell site data is collected regularly in such a manner, it is not within the scope of information a pen register is authorized to obtain.

3. STORED COMMUNICATIONS ACT

[68] The Stored Communications Act provides authority to obtain "Stored Wire and Electronic Communications and Transactional Records

[175] *See, e.g., Texas Decision*, 396 F. Supp. 2d at 765.
[176] One court has in fact already found that the authority of the Pen Register statute, by itself, is enough to obtain prospective cell site data. West Virginia Decision, 415 F. Supp. 2d 663 (S.D. W.Va. 2006), discussed further in Section IV(D), *supra*.
[177] 18 U.S.C. § 3127(3).
[178] This author has spoken with two engineers in the cellular technology field about this issue, one of whom works for Nortel Networks and the other for a major Canadian cellular technology provider. Each stated that he knew of several cellular service providers who record at least some cell cite data for billing and quality-assurance purposes. [Names withheld on request].

Access."[179] Under the SCA, stored records are split into three categories: (1) Stored communications stored less than 180 days; (2) stored communications stored more than 180 days; and (3) transactional and subscriber information.[180] Since the SCA adopts the definition of "contents" from the Wiretap Act and since cell site data is not "contents" under the Wiretap Act, the first two categories of stored communications are irrelevant for this analysis.[181] The government may obtain "subscriber" information using a simple administrative subpoena; however, subscriber information is limited to six narrow categories of information, none of which are related to cell site data.[182]

[69] The final category of records under the SCA protects "transactional" records or "[r]ecords concerning electronic communication service or remote computing service."[183] An "electronic communication service" is "any service which provides users thereof the ability to send or receive wire or electronic communications."[184] An "electronic communication" has the same definition as in the Wiretap Act.[185] This very broad definition includes transfers of "signals," "images" or "data" through "radio," which would seem to include cellular voice and data communications.[186] Thus the SCA covers transactional records from cellular service providers.[187]

[70] The next step is to determine what records are actually covered under the transactional records section of the SCA. The legislative history shows that transactional records comprise "information about the customer's use of the service" other than the content of the user's

[179] This is the official title of Chapter 121 of Title 18 of the United States Code.
[180] 18 U.S.C. § 2703.
[181] 18 U.S.C. § 2711(1) (adopting, by reference, the definitions from the Wiretap Act, 18 U.S.C. § 2510); Texas Decision, 396 F. Supp. 2d 747, 758 (S.D. Tex. 2005).
[182] 18 U.S.C. § 2703(c)(2); *Texas Decision,* 396 F. Supp. 2d at 758.
[183] 18 U.S.C. § 2703(c)(2).
[184] 18 U.S.C. § 2510(15).
[185] *See supra* note 146.
[186] 18 U.S.C. § 2510(15). This definition also excludes tracking device communications, but this is irrelevant since I have rejected the notion that the acquisition of cell site data turns a cellular telephone into a "tracking device" whose "communications" are the cell site data. *See supra* note 148.
[187] *Texas Decision,* 396 F. Supp. 2d at 758.

communications.[188] One court, addressing the scope of 18 U.S.C. § 2709 (covering FBI counterintelligence access to *subscriber and transactional records*), concluded that Section 2709 "does not require communication service providers to create records which they do not maintain in the ordinary course of business."[189] While this case describes the scope of the term "telephone toll billing records," the same reasoning should apply to transactional records under Section 2703(c) – that is, the government may obtain through a Section 2703(c)(1) order only records that the cellular service provider creates and maintains in the ordinary course of business.[190]

[71] Under this reasoning, the government should be able to obtain *historical* cell site data under Section 2703(c)(1) so long as that information is regularly created and maintained in the ordinary course of business. Recent court decisions and publicly available documents do not specifically indicate how much data is recorded and how long that data is maintained. However, it is clear that at least some cellular providers record and maintain cell site data since such data has been used in a variety of cases already.[191] Cellular providers most likely keep at least

[188] S. Rep. No. 99-541, at 38, *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592; *Texas Decision,* 396 F. Supp. 2d at 758.

[189] *In Re* Matter of Grand Jury Subpoenas to Southwestern Bell Mobile Systems, 894 F.Supp 355, 348-49 (W.D. Mo. 1995). There is nothing to suggest that the subscriber and transactional data covered under 18 U.S.C. § 2709 is any different than that covered under Section 2703(c).

[190] *See, e.g.,* Freiwald Memo, *supra* note 168, at 5-6 (discussing *In re* Grand Jury Subpoena to Southwestern Bell Mobile Systems, Inc., 894 F. Supp. 355 (W.D. Mo. 1995), and the applicability of the legislative history of Section 2709 to 2703.)

[191] *See, e.g.,* People v. Stovall, No. B172771, 2005 WL 977733 (Cal. Ct. App. April 28, 2005) (expert testimony regarding suspect's location at time of murder based upon Verizon billing records showing defendant had made and received several calls using two cell sites in the vicinity of the murder location); People v. Pese, No. A100933, 2004 WL 899768 (Cal. Ct. App. April 28, 2004) (cell phone records showed defendant made several calls using cell sites in vicinity of the location where victim's body was found). *See also* examples in *Who Knows Where You've Been supra* note 15, at 310-12. The author has worked on a large federal RICO conspiracy case where the government had obtained historical cell site records and planned to use such records as evidence that one or more defendants were in the vicinity of a crime scene. The author has also heard anecdotal evidence from several criminal defense attorneys who regularly represent clients in federal court that the U.S. Attorney's Office regularly obtains such information for use as evidence at trial in serious felony cases.

some of this information for later analysis in determining trends in usage in order to determine the best methods of routing and where additional cell site towers are required.[192]

[72] Unfortunately for the government, the structure and plain text (and title) of the SCA show that it is of a purely historical nature and therefore unfit for authorizing the acquisition of prospective and/or real-time records. As noted by several courts, the SCA needs to be examined as part of the overall surveillance scheme setup by the ECPA.[193] The Wiretap Act and the Pen Register Provisions necessarily cover real-time (or at least prospective) access to data, since they require "interception" – which has been construed by several courts to mean acquisition contemporaneous (or at least nearly contemporaneous) with transmission.[194] Because they are prospective in nature, both the Wiretap Act and the Pen Register Provisions require that interception be authorized only for a limited time and because they reflect on-going investigations, they are at least temporarily sealed.[195] In contrast, the SCA has no time limitations of any sort (other than relating to the standard required for obtaining the contents of stored communications stored for more or less than 180 days). Thus, the plain statutory language of the SCA and the statutory scheme in which it was created show that the SCA was meant to cover the acquisition of solely *retrospective* – and not *prospective* – data.[196]

[73] One final issue is worth discussing in the context of the SCA: The blurring of the line between "records" and "real-time" data. If the government can obtain historical cell site data using an SCA order, what prevents the government from obtaining a new order every week, every day, or even every hour to obtain any records which have been created in

[192] T-Mobile's own Privacy Notice contemplates future potential use of cell site data for commercial/advertising and service-related uses. *See What About Location-Based Services and Information*, T-Mobile, Privacy Notice, http://support.t-mobile.com/knowbase/root/public/tm22030.htm, (last accessed May 9, 2007).
[193] *See, e.g.*, *Texas Decision,* 396 F. Supp. 2d at 760.
[194] U.S. v. Steiger, 318 F.3d 1039,1048-49 (11th Cir. 2003); Konop v. Hawaiian Airlines, 302 F.3d 868, 878 (9th Cir. 2002); Steven Jackson Games v. U.S. Secret Service, 36 F.3d 457, 463 n. 8 (5th Cir. 1994).
[195] 18 U.S.C. §§ 2518(5), (8)(b) (1993 & Supp. 2006); 18 U.S.C. § 3123(c) (1993 & Supp. 2006).
[196] *Texas Decision,* 396 F. Supp. 2d at 760.

the time since the last order?[197] Electronic information is converted into a "record" almost immediately. If the service provider regularly keeps those "records," what does the "pen register" device actually do? Is it merely a piece of software that waits for new records to be created and transmits the new records to law enforcement on an ongoing basis? Or does it actually "intercept" the data before it becomes a record and then send that information to law enforcement? These questions remain unanswered. For the purposes of this paper, it is sufficient to note that, while the statutory language of the SCA may allow repeated orders on even an hourly basis, at some point a court is likely to enforce the spirit of the ECPA by finding this practice to be a de facto "interception."

4. TRACKING DEVICE STATUTE

[74] Several court decisions have cited the Tracking Device Statute as a potential source of authority for obtaining an order authorizing the acquisition of real-time cell site data.[198] While at first blush it seems like the most logical match, in reality the Tracking Device Statute does not *authorize* anything and is merely a left-over statute.

[75] Prior to the passage of the Tracking Device Statute, Federal Rules of Criminal Procedure Rule 41 did not expressly authorize the monitoring of a tracking device *outside* of the jurisdiction which had authorized the order.[199] The Tracking Device Statute thus clarified that, where a court was *already* empowered to grant a warrant for the installation of a tracking device, it could also authorize the monitoring of the tracking device outside of that jurisdiction.[200] Since that time, Rule 41 has been amended to allow exactly what the Tracking Device Statute authorized.[201]

[76] Additionally, as several courts have noted, the Tracking Device Statute "does not *prohibit* the use of a tracking device in the absence of conformity with the section . . . [n]or does it bar the use of evidence

[197] S.D.N.Y. Decision I, 405 F. Supp. 2d 435, 448 (S.D.N.Y. 2005).
[198] *See, e.g.,* E.D.N.Y. Decision II, 396 F.Supp. 2d 294, 391 (E.D.N.Y. 2005); *Texas Decision*, 396 F. Supp. 2d at 743.
[199] *See* United States v. Gbemisola, 225 F.3d 753, 758 n. 2 (D.C. Cir. 2000); FED. R. CRIM. P. 41; Lee, *supra* note 15 at 395.
[200] *Gbemisola*, 225 F.3d at 758 n. 2*;* 18 U.S.C. § 3117 (1993 & Supp. 2006).
[201] *Gbemisola*, 225 F.3d at 758 n. 2; FED. R. CRIM. P. 41.

acquired without a [Tracking Device Statute] order."[202] The *Gbemisola* court examined the legislative history of the statute and found that Congress was aware that the *Knotts* holding allowed warrantless installation and monitoring of a tracking device on public highways.[203] Congress therefore knew of the lax constitutional limitations on the use of tracking devices in non-constitutionally-protected areas but did not expand the constitutional protection, other than to broaden the jurisdictional reach of a warrant.

[77] The government has argued in several cases that cell site data is so imprecise that it does not "permit the tracking of the movement of a person or objective."[204] Any discussion of the precision or accuracy of cell site data in determining location in the context of the Tracking Device Statute is irrelevant for several reasons. First, neither the plain language of the statute, nor the legislative history say anything about accuracy.[205] Second, technology is progressing at such a quick pace that any arguments that cell site data is not precise enough to count as a tracking device will soon become moot, if they are not already.[206] Third, the fact that the government seeks the cell site data at all shows it is accurate enough to be of use (whether evidentiary or otherwise) to the government.

[78] The Tracking Device Statute neither sets a requirement for the installation and monitoring of a tracking device, nor does it expand the constitutional protection against the use of tracking devices. As a result, it is not really a part of the statutory "scheme" setup by the ECPA and is therefore irrelevant to determining the proper standard the government must meet in order to obtain real-time cell site data.

---

[202] *See, e.g., Gbemisola,* 225 F.3d at 758; Forest*, supra* note 66, at 950 (quoting *Gbemisola*).
[203] *Gbemisola*, 225 F.3d at 758 (quoting H.R. Rep. No. 99-647, at 60 (1986)).
[204] Maryland Decision I, 402 F. Supp. 2d 597, 603 (D. Md. 2005). *See also* Texas Decision, 396 F. Supp. 2d 747, 755 (S.D. Tex. 2005) ("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.").
[205] *See* 18 U.S.C. § 3117 (2006).
[206] *Maryland Decision I,* 402 F. Supp. 2d at 599, n. 4.

5. COMBINED AUTHORITY OF PEN REGISTER PROVISIONS AND STORED COMMUNICATIONS ACT

[79] Having determined that neither the Pen Register Provisions nor the SCA, by themselves, authorize the acquisition of prospective cell site data, I now turn to the "hybrid theory" set forth by the government in the several cases discussed above in Section IV. The "hybrid theory" asserts that, while Section 1002 prohibits the acquisition of prospective cell site data "solely pursuant to" the Pen Register Provisions, the government merely needs to add some additional authority in order to get over the hurdle set up by Section 1002.[207] The government has contended that the SCA provides such additional authority.[208]

[80] Combining two statutes, neither of which individually authorizes something, to obtain the authority to authorize that thing is a novel idea. One commentator has attacked this theory on the grounds that "0 + 0 = 0".[209] The government, in support of its hybrid theory, has never cited another similar arrangement, where two independent statutes are combined to obtain a result that neither authorizes separately.[210] This "hybrid theory" is distinguishable from the regular practice of law enforcement of combining applications and orders for separate results. For instance, combining a Pen Register application and order in the same packet as a SCA application and order to obtain (respectively) the results of a pen register and some stored records is not problematic. In that situation, the Pen Register Provisions independently provides the authority to obtain numbers dialed, whereas the SCA independently provides the authority to obtain stored records.

---

[207] *See, e.g., id.* at 603.
[208] *Id*.
[209] Freiwald Memo, *supra* note 168. *See also* Press Release, Electronic Frontier Foundation, New Case Reveals Routine Abuse of Government Surveillance Powers: Cell Phones Used to Track Users Without Probable Cause (Sept. 26, 2005) ("It's as if the government wants the court to believe that zero plus zero somehow equals one."), *available at*, http://www.eff.org/news/archives/2005_09.php#004002.
[210] *See, e.g.,* Texas Decision, 396 F. Supp. 2d 747, 764-65 (S.D. Tex. 2005) ("[N]o other form of electronic surveillance has the mixed statutory parentage that prospective cell site data is claimed to have.")

[81] Even more problematic, while they were originally enacted concurrently, the SCA and the Pen Register Provisions make no cross-references to each other.[211] The 1986 Congress which passed the ECPA must have known how to cross-reference statutes when needed, as it cross-referenced both the Pen Register Provisions and the SCA with the Wiretap Act.[212] If that Congress had meant for the two statutory schemes to be combined to obtain something neither authorized independently, it seems likely that Congress would have done so at that time.[213] When CALEA amended the statutory scheme by adding Section 1002, it did so without adding any reference in Section 1002 to the SCA. Presumably, the 1994 Congress which passed CALEA would have explicitly made such a reference if had meant the term "*solely pursuant to* [the Pen Register Provisions]" to mean, without additional authority provided by the SCA.[214] The more likely scenario is that Congress meant to leave the door open for a later statute which would authorize the acquisition of cell site data by the technical device known as a pen register but using a different standard. Since the SCA existed in 1994 and its scope has not been enlarged enough since then to independently authorize the acquisition of real-time cell site data, the 1994 Congress simply could not have meant the SCA to provide the extra authority required under Section 1002.

[82] Much has been said by courts and commentators about the testimony of then-FBI Director Louis Freeh during the congressional hearings on CALEA.[215] Freeh testified that CALEA was not meant to "enlarge or reduce the government's authority" but merely to "maintain[] the status quo".[216] If CALEA was meant to protect the status quo, and prior to its

[211] *Id.* at 764.
[212] *See* 18 U.S.C. § 2711(1) (2006) (adopting, by reference, the definitions from the Wiretap Act, 18 U.S.C. § 2510); 18 U.S.C. § 3127(1) (adopting, by reference, several definitions from the Wiretap Act, 18 U.S.C. § 2510).
[213] *Texas Decision*, 396 F. Supp. 2d at 764-65 (noting that "[i]f 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.")
[214] *Id*. at 757 (emphasis added).
[215] *See, e.g.*, Freiwald, *supra* note 47, at 979-80; *Texas Decision*, 396 F. Supp. 2d at 763-65; E.D.N.Y. Decision II, 396 F. Supp. 2d 294, 319 (E.D.N.Y. 2005).
[216] *Texas Decision*, 396 F. Supp. 2d at 763 (quoting from Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings Before the Subcomm. on Technology and Law of

passage the status quo included no device whereby the SCA and Pen Register Provisions could be combined to obtain prospective cell site data, it is hard to see how Section 1002 could authorize this new combination. For the purposes of this paper, it is enough to merely recognize that Freeh never suggested that the Pen Register Provisions could be combined with another statute to obtain prospective cell site data, nor do the congressional reports on CALEA mention such a combination.

[83] Thus, the plain language of the statutes, the structure of the statutory scheme, and common sense show that the "hybrid theory," that is the combination of the authority of the Pen Register Provisions and the authority of the SCA to obtain prospective cell site data, is unsupported by the law.

6. COMBINED AUTHORITY OF PEN REGISTER PROVISIONS AND RULE 41 WARRANT

[84] The final means of obtaining prospective cell site data is to use a Rule 41 warrant. Most of the courts addressing this issue have required the government to bring an application for a Rule 41 warrant with the requisite probable cause showing in order to obtain prospective cell site data.[217] Rule 41 allows a law enforcement officer to obtain a warrant for:

> (1) evidence of a crime;
> (2) contraband, fruits of crime, or other items illegally possessed;
> (3) property designed for use, intended for use, or used in committing a crime; or
> (4) a person to be arrested or a person who is unlawfully restrained.[218]

[85] In order to obtain a warrant, law enforcement must present evidence (through an affidavit or testimony) showing probable cause.[219] Of the four

---

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)).

[217] *See, e.g., Texas Decision*, 396 F.Supp.2d at 765 ; *E.D.N.Y. Decision II*, 396 F.Supp. at 326-27; Maryland Decision I, 402 F. Supp. 2d 597, 605 (D. Md. 2005); W.D.N.Y. Decision, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006).

[218] FED. R. CRIM. P. 41(C).

types of warrants, cell site data fits only one category: evidence of a crime. There is nothing in the ECPA or any other federal statute which prohibits the use of a warrant to obtain cell site data.

[86] Law enforcement does not, however, seem able to obtain cell site data by itself, but must obtain it through the cellular provider. To obtain cell site data, law enforcement officers need an order requiring the cellular provider to provide them with such information. A warrant merely allows the search and seizure of evidence. A warrant would allow a law enforcement officer to enter the premises and obtain the information directly from the cellular provider. On the other hand, cellular providers can easily comply with a warrant for prospective cell site data by simply installing a piece of software which is, in essence, a pen register.

[87] For all practical purposes, then, a Rule 41 warrant authorizing the search and seizure of cell site data for an individual is merely an order to the cellular provider to install its own pen register and send the results to law enforcement. For this reason, the government may find it advantageous to apply for both a warrant and a pen register order at the same time, with the warrant providing the authority to use the pen register for the acquisition of prospective cell site data. Ultimately, the government's "hybrid theory" is correct, except that the additional authority required by Section 1002 is a Rule 41 warrant. The difference in the "hybrid theory" here is that, whereas neither the SCA nor the Pen Register Provisions provide the authority to obtain the *results* (prospective cell site data), here the warrant provides the authority to obtain the *results*, and the Pen Register Provisions merely provides a *physical device or means* for obtaining that result.

7. SUMMARY

[88] The Wiretap Act does not provide the authority for obtaining cell site data because it applies solely to "contents" of communications, and cell site data is not the "contents" of a communication. The Pen Register Provisions do seem to provide the authority for obtaining cell site data, except for the fact that Section 1002 explicitly precludes the Pen Register Provisions from providing that authority. The Stored Communications

[219] FED. R. CRIM. P. 41(D).

Act provides the authority for obtaining *historical* cell site data that cellular providers regularly keep, but given its plain language and its context within the larger statutory structure of the ECPA, it cannot provide the authority for obtaining *prospective* cell site data. The Tracking Device Statute is neither mandatory nor prohibits the installation and monitoring of tracking devices. The Tracking Device Statute itself merely clarified a hole in Federal Rules of Criminal Procedure Rule 41 which has since been filled. The combination of the Pen Register Provisions and the SCA is not enough to obtain prospective cell site data since neither statute separately provides sufficient authority to obtain such data. Moreover, the legislative history and the structure of the statutes do not support the contention that Congress ever meant for such a combination of authority. Finally, a Rule 41 warrant provides sufficient authority to obtain prospective cell site data. A cellular provider is likely to implement a Rule 41 warrant for cell site data through the use of a device like a pen register, so law enforcement should combine a Rule 41 warrant application with a pen register application and order.

C. CONSTITUTIONAL ANALYSIS

[89] Separate from the statutory issue is the issue of whether the acquisition of prospective cell phone tracking data implicates the protections of the Fourth Amendment. Prospective cell site data implicates two separate levels of Fourth Amendment analysis: (1) Whether the cell phone user retains a reasonable expectation of privacy in his cell site data; and (2) whether a cell phone user has a reasonable expectation of privacy in his location in a public or private place.

[90] The Fourth Amendment protects individuals from searches and seizures where that individual has a subjective expectation of privacy and that expectation of privacy is objectively reasonable.[220] *Knotts* and *Karo* together hold that, while a person has no reasonable expectation of privacy in their location while in a public place, that person does retain a reasonable expectation of privacy in their location once they enter into a home.[221] More recently, the Supreme Court reinforced the notion of the

[220] Katz v. United States, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).
[221] United States v. Knotts, 460 U.S. 276, 281 (1983); United States v. Karo, 468 U.S. 705, 714 (1984).

home as a special constitutionally-protected zone in holding that a sense-enhancing device constituted a search, notwithstanding that the device never intruded into the home.[222]

[91] On the other hand, the Supreme Court has held that warrantless interception of telephone numbers dialed does not violate the Fourth Amendment.[223] This is because, the court reasoned, a person could have no objectively reasonable expectation of privacy in information (in that case, the telephone numbers) which has been "voluntarily conveyed" to a third party (there the telephone company), and the subscriber knows that the telephone company can and does record those numbers.[224]

[92] The government has argued, relying on *Smith v. Maryland*, that cell site data does not implicate the Fourth Amendment because, like telephone numbers, it is "voluntarily conveyed."[225] The problem with this argument is that, unlike telephone numbers which the user must actively dial and send to the telephone company, cell site tracking data is automatically transmitted, regardless of whether the person is using the cell phone at the time.[226] This information must be transmitted in order to use the device because the device must always communicate with a particular cell tower in order to receive incoming calls or make outgoing calls.[227] Cell site data is not information which the user contemplates sending when walking or driving around with a cell phone, nor does the user ever enter this information himself, as is the case with telephone numbers. Additionally, few cellular phone users are likely to know that their movements can be tracked with substantial accuracy at any time their cellular phones are turned on.[228] Thus cell phone users seem to retain a subjective expectation of privacy.

---

[222] United States v. Kyllo, 533 U.S. 27, 34 (2001).
[223] Smith v. Maryland, 442 U.S. 735, 744 (1979).
[224] *Id*.
[225] *See* Texas Decision, 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005).
[226] *Id.* at 756-57.
[227] *Id.* at 750-51.
[228] It is true that many cell phone users may know that their location can be tracked when they dial 911 or, if they have enabled specialize software, through GPS – but most cell phone users do not know they can be tracked *whenever* their phone is on. *See Id.* at 757.

[93] It could also be argued, relying on *Knotts* and *Karo*, that the Fourth Amendment is not violated by warrantless acquisition of prospective cell site data since it does not provide sufficiently accurate or precise information to show whether a person is inside a residence or in a public place.[229] While this may or may not be true under current technology, it will not remain that way. Technology advances at such a fast pace that legislation and even court decisions often cannot keep up.[230] Triangulation techniques and GPS technology are likely to continually improve to the point where law enforcement may be able to determine a person's exact location within a residence.[231] Even today, if the government seeks GPS information (which may or may not be transmitted automatically on a regular basis) from a cell phone handset the government may be able to determine the location of that handset within the home with a high degree of accuracy.[232]

[94] An argument can also be made that users have an objectively reasonable expectation of privacy in their cell site data due to privacy clauses in cellular service contracts and privacy policies. For instance, T-Mobile's current Privacy Notice states that T-Mobile only discloses "location information [cell site data] to third parties when *required* to do so," such as during emergency situations (when user has dialed 911), to law enforcement, or to a user's guardian or immediate family members in emergency situations.[233] Verizon Wireless goes further by stating, "We support notice and informed consent for the use of any personally identifiable wireless location and transactional information [cell site data]. We will not store this type of information beyond its normal useful life,

[229] *Id*. at 755.
[230] Maryland Decision I, 402 F. Supp. 2d 597, 599 (D. Md. 2005).
[231] *Id*.
[232] Differential GPS technology provides accuracy of within one to three meters, precise enough to determine someone's location even within a very small home. *See* U.S. Department of Transportation Federal Highway Administration, *Nationwide Differential Global Positioning System Program Fact Sheet*, *available at* http://www.tfhrc.gov/its/ndgps/02072.htm (last visited May 9, 2007).
[233] T-Mobile, Privacy Notice, *available at* http://support.t-mobile.com/knowbase/root/public/tm22030.htm (last visited May 9, 2007) (emphasis added). *But see* Nextel, Privacy Police – Presence, Location, and Tracking Information, *available at* http://www.sprint.com/legal/nextel_privacy.html#presence (last visited May 9, 2007) (merely listing the uses to which Nextel currently uses location information, and not limiting any use beyond that).

including for internal service evaluation and quality assurance purposes, except as required by law."[234]

[95] These privacy policies must be balanced against the [mis]-information users obtain from television and film. Films and TV programs, such as "CSI," "24," and "Enemy of the State" occasionally show government agencies tracking users quite accurately via their cell phones. Since the films are purely fictional and end users have at least constructive notice of the cellular privacy notices, I believe users do have a reasonable expectation of privacy in their cell site data.

[96] Ultimately the government is correct that a cell phone user has no reasonable expectation of privacy in his location in a public place. However, because a cellular phone user retains a reasonable expectation of privacy in his cell site data, and because technology will soon improve to the point where cell site data is likely to show a person's location within a home, this argument is immaterial: Obtaining prospective cell site data without a warrant is, or at least soon will be, a violation of the 4th Amendment.

D. SUMMARY

[97] The statutory scheme setup by the ECPA does not directly address the acquisition of prospective cell site data. The Wiretap Act covers only "contents" of communications and cell site data is not "contents." The Pen Register Provisions seem to cover prospective cell site data, but cell site data is exempt from its coverage by CALEA. The SCA covers historical cell site data but not prospective cell site data. The "hybrid theory" – using the combined authority of the Pen Register Provisions and the SCA – is flawed because neither statute provides the requisite authority by itself for acquiring prospective cell site data and there is no indication that Congress meant for these two statutes to be combined for this purpose. Therefore, because the government seeks an order, the default is a Rule 41 warrant. A Rule 41 warrant authorizes the acquisition of prospective cell site data. A Rule 41 warrant can also be combined

[234] Verizon Wireless Privacy Principles, *available at* http://www.verizonwireless.com (follow "Privacy" hyperlink; then follow "Privacy Principles" hyperlink)(last visited May 9, 2007).

with a pen register application and order to use the *mechanism* of the physical pen register device to obtain the *results* authorized by the Rule 41 warrant.

[98] The Fourth Amendment does provide some limits on the acquisition of prospective cell site data. Because cell site data is not actively given over to the cellular provider through affirmative acts of the cellular phone user, cell site data is not "voluntarily conveyed" to the cellular provider. Thus a cellular phone user retains a reasonable expectation of privacy in his cell site data. Any argument that the accuracy of existing technology prevents the government from determining an individual's location within a residence is a short-term technology-specific argument which will become moot in the near future as technology improves. Moreover, cellular privacy policies enforce the users' reasonable expectation of privacy.

[99] In sum, where law enforcement seeks to obtain an order authorizing the acquisition of prospective cell site data, it can do so only through a showing, under Federal Rules of Criminal Procedure Rule 41, of probable cause to believe the prospective cell site data is evidence of a crime. Any warrantless acquisition of prospective cell site data, whether through a "hybrid theory" order or merely without any order, is unsupported by law and likely to run afoul of the Fourth Amendment.

VI. CONCLUSION

[100] In this paper, I have examined law enforcement acquisition of prospective cell site data by first describing the relevant cellular tracking technology and related regulation, then examining the statutory schemes and case law regarding electronic surveillance and cell site data prior to 2005, and finally analyzing the recent cases directly addressing the government's "hybrid theory" for obtaining prospective cell site data.

[101] I have concluded that under the current statutory scheme, the government must obtain a Rule 41 warrant in order to acquire prospective cell site data, whereas it need only obtain a SCA order to acquire historical cell site data. In addition to the statutory limitations, the Fourth Amendment is also likely to impose restrictions on how and when law enforcement may acquire prospective cell site data.

[102] The cell phone has become an important part of everyday life for many Americans and has the potential to improve the lives of many people. Innovation in cellular technology and cell phone usage may be stifled, however, if government overreaching and ambiguities in electronic surveillance law scare away end users. The confusing state of electronic surveillance law relating to cell site data contributes to legal ambiguity and leaves the system open to abuse. Moreover, abuse of the system could lead to a form of the Panopticon that even Jeremy Bentham himself could not have imagined. Congress should step in to regulate the acquisition of prospective cell site data in order prevent abuse and encourage innovation in and adoption of cellular technology.