Volume 41
Number 4 *Symposium on Electronic Privacy in the Information Age*
*pp.*1543-1586

Symposium on Electronic Privacy in the Information Age

A Probable Nightmare: Lifting the Fog from the Cellular Surveillance Statutory Catastrophe

Rickey G. Glover

A PROBABLE NIGHTMARE: LIFTING THE FOG FROM THE CELLULAR SURVEILLANCE STATUTORY CATASTROPHE†

I. INTRODUCTION

"BIG BROTHER IS WATCHING YOU"[1]

Though far from the icy Orwellian description of Oceania, the ever-increasing technological advancements of American society create powerful tools allowing law enforcement unprecedented ability to locate individuals based on the mechanics of electronic information transmission.[2] Inherent in the ability of law enforcement to easily track individuals is the encroachment upon the individual privacy rights of those tracked.[3] For over two decades, law enforcement officials have used information gathered from cellular telephone companies to track individuals based on cell phone usage.[4] Further, prosecutors have routinely requested, and have been granted, forms of real time tracking information from third party service providers without the need for a showing of probable cause.[5] Perhaps due to the growing specificity with

† Winner of the 2007 Valparaiso University Law Review's Scribes Award

1 George Orwell, Nineteen Eighty-Four 3 (1949).

2 *See, e.g.*, Steven V. Treglia, *The Challenge of Tracking: Difficult Times May be Ahead for U.S. Legal System*, N.Y.L.J., Jan. 17, 2006, at 50 [hereinafter Treglia, *Challenge of Tracking*] (discussing the increasing specificity with which law enforcement can pinpoint any individual's whereabouts by obtaining cell site information and the confusion that results from enforcing twenty-first century technology with eighteenth-century legal analysis).

3 *See* Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1429 (2004). Blitz, building on the thoughts of fellow academics, posits that when the "architecture of privacy begins to break down under pressure from new surveillance technologies, courts can do two things to restore their privacy-protecting functions." *Id.* First, laws can be changed to keep the government at bay. *Id.* Second, and perhaps more importantly, legal changes that effectively limit government access to information society deems private may encourage others, like law enforcement agencies, "to build such constitutional limits into the technology of surveillance they use or the procedures for using it." *Id.* at 1430; *see also* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 8-24 (1999) (discussing the impossibility of curbing the flood of technology and the resulting need of society to ensure that the power gained therefrom is utilized democratically).

4 *See* Steven V. Treglia, *Trailing Cell Phones: Courts Grapple with Requests from Prosecutors Seeking Prospective Tracking*, N.Y.L.J., July 18, 2006, at 5 [hereinafter Treglia, *Trailing Cell Phones*] (describing the recent cases dealing with prospective cell site information requests and giving a brief history of the statutory framework guiding law enforcement tracking analysis).

5 *Id.*; *see also In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) [hereinafter SDTX#1] (referring to the practice of combining a request for subscriber information with an

which an individual's whereabouts can be determined, recent courts have taken on the weighty challenge of reassessing the showing required for law enforcement to obtain prospective, real time[6] cell site information from cellular service providers.[7] Instead of clarifying the requisite

---

application to install a pen register and trap/trace device as "standard practice," which requires a showing of specific and articulable facts and certified relevance respectively).

[6] For purposes of this Note, the terms "prospective" and "real time" have the same meaning when in reference to cell site information. Specifically, the terms refer to that information acquired by the government *after* a court order, authorizing the government to obtain cell site information from a third party service provider has been signed. The terms do not refer, however, to information deemed historical, or to information stored by a third party service provider detailing the location of a specific cell phone in the past. An example of prospective or real time cell site information is a registration signal transmitted from a cellular phone, obtained by the government from a third party service provider pursuant to a court order. An example of historical information is a third party record of a user's whereabouts for the purpose of determining roaming charges.

[7] *See, e.g.*, *SDTX#1*, 396 F. Supp. 2d at 765 (requiring a showing of probable cause); *In re* the Application of U.S.A. for an Order Authorizing the Installation and Use of a Pen Register with Caller Identification Device and Cell Site Location Authority on a Certain Cellular Telephone, 415 F. Supp. 2d 663 (S.D. W. Va. 2006) [hereinafter SDWVA] (allowing limited real time information with a showing of only specific and articulable facts).

Congress actually demanded enhanced tracking in 1997, when it attempted to extend to cellular phones the 911 dialing services available to wired phones. *See* 47 C.F.R. § 20.18 (2006). The first phase of the plan required third party service providers to forward all 911 calls to the appropriate Public Safety Answering Point. *Id*. § 20.18(d)(1). Further, third party providers were required to develop technology allowing the location of individual mobile phones through cell site information. *See* Matthew Mickle Werdegar, Note, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, STAN. L. & POL'Y REV., Fall 1998, at 103, 105 (discussing the FCC 911 Act).

Phase II required third party mobile service providers to have the capability to locate the latitude and longitude of 67% of cellular phones within a radius of fifty meters and 95% of cellular telephones within a radius of 150 meters. 47 C.F.R. § 20.18(h)(2). For the remaining 5% of cellular telephone 911 calls, Phase II required the third party service provider to attempt location and provide that information to the appropriate Public Safety Answering Point. 47 C.F.R. § 20.18(h)(3); *see also* David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communication*, COMM. L. & POL'Y, Winter 2003, at 3 (discussing government motivation for cell phone tracking capabilities). Phillips states:

> In the United States, a primary motivating force behind wireless surveillance is the implementation of emergency response systems. These systems were originally designed to provide a single, easy-to-remember phone number—911—which would route all police, fire and other emergency calls to a central public safety answering point (PSAP) which would then dispatch the call to the appropriate response team.

Id. Further, Global Positioning Systems ("GPS") have greatly enhanced the ability to pinpoint a particular mobile telephone. *Treglia, Challenge of Tracking*, *supra* note 2, at 1 (noting the increasing specificity with which personal identification based on cell usage is possible). Of course, in more rural areas with less cell sites, the ability to pinpoint an individual mobile phone is greatly reduced; however, in urban areas, triangulation based

showing, however, the resulting jurisprudence confused an already difficult area of technology law.[8] To illustrate, consider the following.[9]

Detective Doe received a call at approximately 12:00 a.m. A robbery had taken place at a grocery store on the north side of town. The robber, identified by a seventy-five year old witness as a "larger black man, driving a big yellow car" took nearly two hundred dollars from the cash register before fatally wounding the store clerk. Upon arrival, Detective Doe viewed the grainy surveillance video taken by a camera at the back of the store. Due to the overly frugal tendencies of the shopkeeper, this particular video had been through the machine continuously for the past two years. Doe was, however, able to make out the man as a black male, age 35-40, approximately 6'1" tall, wearing a dark jacket and jeans. He also caught a glimpse of the yellow car as it sped away from the scene, a car the Detective thought to be a 1975 Ford Cortina.

Discouraged, Doe dialed police headquarters.

"I need a list of all yellow 1975 Ford Cortinas registered in the state," Doe snapped.

Earlier that night, Cameron Smith lay awake next to his wife Cheryl, their two-month old baby resting in the bassinet next to her. He gazed at his beautiful family, gently sleeping, and said a prayer of thanks for his blessings. He then turned, checking once again that his phone was set to wake him for his trip. Satisfied, he placed his arm around Cheryl and drifted off to sleep.

An hour later, while Cameron slept calmly, a man, approximately 6'1" tall, wearing a dark jacket and jeans, entered the carport of a house sixty miles away from Cameron's. The man quietly slipped a metal rod into the driver's side door of the bright yellow car. First applying pressure and then slightly lifting, the man managed to guide the silver lock with ease. His next step, grab some quick cash before making a

---

on multiple cell sites can produce staggering specificity, giving prosecutors and other government officials a virtual map of a suspect's movement and a powerful tool for apprehending suspects. *Id.* Finally, due to continuous mobile phone network registration (discussed *infra* notes 30-33 and accompanying text), cell phone tracking is easily accomplished without the customer knowing she is being tracked. *Id.*

[8] *See* Treglia, *Trailing Cell Phones*, *supra* note 4 (discussing the district split, the minority position requiring a showing of specific and articulable facts, and the majority position requiring a showing of probable cause).

[9] The following hypothetical is completely fictional and the creation of the author entirely. Any resemblance to real persons or facts is coincidental.

break for the border. But, as these things usually go, an unusually disobedient store clerk interrupted his plan. The man had to act quickly; he decided to ditch the car, wipe it down, and run as far as possible.

Detective Doe had been working all night. At 4:30 a.m., he had received the list of nine cars meeting his description. Annoyed and knowing that the killer could be anywhere by now, he searched the public records to find if any of the car owners had cellular phones. He saw that each of them did, and, as per custom with possible interstate flight, he wrote up a request that the federal magistrate judge grant him access to all cell site information for each of the phones. Knowing that he only needed to show the records were relevant and material to the investigation, Detective Doe was not discouraged that he was basing his entire case theory on a hazy videotape, a weak eyewitness, and his speculative knowledge of automobiles.

At 7:30 a.m., the judge, having been awakened early to sign an expansive order, was not amused. However, he knew that a killer was loose and most likely running. Further, he knew that cellular providers had the ability to pinpoint, with great specificity, the locations of each of their subscribers. The detective had cited authority that seemed to grant the judge the right to sign such an order and the judge did so.

By 8:30 a.m., Cameron, driving his yellow 1975 Ford Cortina, was three hours into his journey. He had to be in Chicago by 1:00 p.m. for a job interview, and the drive from Cincinnati was a long one. Unbeknownst to him, the cell phone in his left pocket was being tracked every seven seconds, creating a virtual map of his movements. Within minutes, he saw lights flashing behind him. He pulled over, cursing himself for getting a late start and speeding through central Indiana. As the officer approached, he reached for the glove box to grab his information. The officer then pointed his gun at Cameron, yelling "freeze" as he quickly approached the car. Cameron, stunned, obeyed the man, who quickly opened the door, slammed him against the car, and cuffed him. The officer, noticing Cameron's skin color and 6' frame, read him his rights and pushed him into his car.

This hypothetical illustrates the problems with our current cellular surveillance statutory framework. Government officials with weak factual foundations are granted the ability to invade individual privacy rights by magistrate judges forced to choose between congressional

intent or cleverly-crafted plain language.[10] The purpose of this Note is to advocate that the current statutory framework must be amended to firmly establish probable cause as the requisite governmental showing necessary to obtain prospective, real time cell site information from third party cellular service providers. Part II of this Note focuses on cellular telephone technology and the background of recent statutory and jurisprudential answers to this growing legal field.[11] Part III of this Note analyzes the two main approaches courts have taken to government requests for real time cell site information: the hybrid theory position, necessitating a showing of specific and articulable facts, and the probable cause position, stemming from the tracking device statute.[12] Part IV of this Note proposes amendments to the Stored Communications Act and the Tracking Device statute that will establish a clear guide for government agents seeking real time cell site information and magistrate judges faced with the decision of whether to grant such requests.[13]

II. BACKGROUND OF STATUTORY AND JURISPRUDENTIAL RESPONSES TO CELLULAR TELEPHONE TECHNOLOGY REQUESTS

> *"Even the Catholic Church of the Middle Ages was tolerant by modern standards. Part of the reason for this was that in the past no government had the power to keep its citizens under constant surveillance. The invention of print, however, made it easier to manipulate public opinion, and the film and the radio carried the process further. With the development of television, and the technical advance which made it possible to receive and transmit simultaneously on the same instrument, private life came to an end."*[14]

---

[10] *See infra* Parts III.A-III.B (analyzing Congress's clear desire for protection of privacy rights and the government's dual authority position, a collection of various statutory parts in conflict with that desire).

[11] *See infra* Part II (discussing cellular telephone technology, the Electronic Communications Privacy Act, Wiretap Act, Stored Communications Act, Pen/Trap Statute, and recent district court real time cell site information decisions).

[12] *See infra* Part III (analyzing the abuse of prosecutorial discretion, the hybrid theory's harm to personal privacy and its disregard of clear congressional intent, and the benefits of the probable cause standard, namely adherence to congressional intent and protection of personal privacy rights).

[13] *See infra* Part IV (suggesting amendments to the current surveillance technology statutory framework, which will serve to establish probable cause as the necessary governmental showing in order to obtain prospective, real time cell site information from third party cellular service providers).

[14] *See* Orwell, *supra* note 1, at 214.

While predicting a totalitarian society controlled by an ever-watchful government, Orwell struck upon a notion that has come to bear in our society. Beyond television, the advent of cellular telephone technology casts a web connecting the world like never before.[15] While society's ability to be present in multiple places at once expands, the government has fought to ensure that its citizens are not unreasonably deprived of essential privacy rights.[16] Below, Part II.A begins with a discussion of basic cell phone technology.[17] Part II.B examines the Electronic Communications Privacy Act of 1986 ("ECPA"),[18] including Title I, which amended the 1968 federal wiretap statute ("The Wiretap Act"),[19] Title II (the "Stored Communications Act" or "SCA"),[20] and Title III (the "Pen/Trap Statute").[21] Finally, Part II.C discusses the current split of authority regarding the showings necessary for the government to gain prospective, real time cell site information from third party cellular service providers.[22]

A. Cell Phone Technology

"Cells" are hexagonal-shaped geographic regions, resembling a grid of honeycombs covering the nation.[23] A "cell site" is a point, generally at the intersection of three hexagonal cells, where base station radio equipment and antennae are located.[24] Each cell site base station has

---

15 *See* Brin, *supra* note 3 (illustrating the flood of cellular technology in the Global marketplace).

16 *See infra* Parts II.B-II.C (discussing the statutory and common law approaches to cellular telephone technology).

17 *See infra* Part II.A (focusing on the frequencies transmitted by cellular telephones, describing cells and cell sites, and describing the registration process).

18 *See infra* Parts II.B.1-II.B.3 (describing each section of the ECPA, the seminal legislation on surveillance technology, and the various levels of proof required by each section).

19 *See infra* Part II.B.1 (examining the Wiretap Act, which deals with the information actually communicated by users over various electronic communications devises).

20 *See infra* Part II.B.2 (discussing the SCA, which deals with communication information stored by various third party service providers and invents the specific and articulable facts standard of proof).

21 *See infra* Part II.B.3 (discussing the Pen/Trap Statute, dealing with non-content information transmitted at the beginning and end of a call).

22 *See infra* Parts II.C.1-II.C.2 (discussing the many district court decisions dealing with prospective, real time cell site information).

23 Tom Farley, *Cellular Telephone Basics*, *Cell and Sector Terminology*, http://www.privateline.com/mt_cellbasics/iii_cell_sector_terminology (last visited Apr. 1, 2007); *see also* S. REP. NO. 99-541, at 8 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3563 (referring to cells as "honeycomb-shaped segments").

24 Farley, *supra* note 23. A common misperception is that cell sites are located within cells transmitting information from a mid-point to the edges of the cell. *Id*. Actually, cell sites are located at intersection points, allowing antennae to send and receive information from three directions, covering three cells. *Id*.

radio equipment that provides coverage for a specified area.[25] When an individual turns on a cell phone, the mobile switch within the phone determines which channel within the cell will carry the conversation.[26] The channel is a paired radio frequency, with one bandwidth utilized by the base station, known as the forward path, and the other by the mobile phone, known as the reverse path.[27] Mobile telephones use two types of channels: control channels, channels that initially set up the conversation, and voice channels, channels that handle either voice, data, or call information.[28] Once a voice channel is established, the reverse path transmits the mobile phone's electronic serial number ("ESN").[29]

Even when not in use by individuals, mobile phones send out registration signals, usually every seven seconds or, when signal strength fails, by way of the reverse path.[30] The registration signals contain, *inter alia*, the mobile phone's ESN, phone number, and home system ID.[31] Data transmitted during the registration process "'[is] not

---

[25] *Id*. The size of the covered area depends, *inter alia*, on "topography, population, and traffic," with even smaller base stations dedicated to coverage of hard to reach areas including "tunnels, subways and specific roadways." *Id*.

[26] Farley, *supra* note 23, at http://www.privateline.com/Cellbasics/Cellbasics03. html. The switch measures signal strength and chooses the channel with the strongest strength within the particular cell, and the phone continues this technique throughout an individual conversation. *Id*. While traveling, if a signal drops below a handover threshold, the base station (on a channel independent of the one dedicated to the conversation) sends a hand-off request to the mobile switch. *Id*. The switch then finds another channel with the greatest available strength. *Id*. The end result is that a single conversation can travel many miles utilizing many cells, cell sites, and channels. *Id*. The FCC allocates frequency space in the U.S. for various radio signals and gives operating licenses to cellular service providers; cellular telephones transmit a frequency of 800 megahertz (specifically running from 824 to 894MHz). *Id*.

[27] *Id*. The channel has a gap in bandwidth, called an offset, which separates the two frequencies. *Id*.

[28] *Id*. Many companies prefer to call control channels "set-up" channels, as that is their primary function. *Id*. It is important to note that the control channel is no longer utilized once the call is established, it merely drops off and the voice channel carries the conversation. *Id*. Further, once the control channel finds a voice channel, the voice channel is responsible for signaling the base station. *Id*.

[29] *Id*. Thus, in sum, a cell phone uses two kinds of channels—control and voice—each of which use two frequencies—forward path (used to send signals to the mobile phone by the base station) and reverse path (used to send signals to the base station from the mobile phone). *Id*. The ESN is a 32 bit number, supplied by the manufacturer, individual to each mobile phone. *Id*.

[30] *Id*. The purpose of the registration is for the cell phone service provider to know the whereabouts of the phone, whether it is roaming or within the home area, and the applicable billing rate according to geographic location of the phone. *Id*.

[31] *Id*. A Texas federal district court, citing the DEPARTMENT OF JUSTICE ELECTRONIC SURVEILLANCE MANUAL, *infra*, described the registration process: "Cellular telephones that are powered on will automatically register or re-register with a cellular tower as the phone

dialed or otherwise controlled by the cellular telephone user.'"[32] Finally, when a person dials a cell phone number, the base station sends a page to the mobile phone via the control channel and assigns a voice channel to the conversation; voice information is then converted into electronic digits, compressed, and transmitted through the voice channel.[33]

B. The Electronic Communications Privacy Act of 1986

In 1983, the Supreme Court held in *United States v. Knotts*[34] that persons traveling in open areas, on public streets, on most private property, or in any location where others could openly observe them had no reasonable expectation of privacy.[35] Further, the Court held that because such individuals had no reasonable expectation of privacy, government monitoring of such individuals was neither a "search" nor a "seizure" as contemplated under the Fourth Amendment.[36] A year later, however, the Court in *United States v. Karo*[37] held, that a showing of probable cause was required for any government tracking within a

---

travels within the provider's service area." SDTX#1, 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) (quoting U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL 178-79 n.41 (2005)). The registration process is the technical means by which the network identifies the subscriber, validates the account, and determines where to route call traffic. *Id*. This exchange occurs on a dedicated control channel that is clearly separate from that used for call content (i.e., audio)—which occurs on a separate dedicated channel. *Id*.

[32] *SDTX#1,* 396 F. Supp. 2d at 751. Registration occurs even when the mobile phone is idle, unbeknownst to its user. *Id*.

[33] *Id*. The court further stated:

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

Id.; *see also* Darren Handler, Note, *An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative*, 10 VA. L.J. & TECH. 1 (2005) (analyzing cell phone technology); Note, *Who Knows Where You've Been: Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 308-16 (2004) (discussing the use of cell phones as law enforcement aids for tracking purposes).

[34] 460 U.S. 276 (1983).

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

[36] *Id.* at 285. "[D]id monitoring the beeper signals complained of by respondent invade any legitimate expectation of privacy on his part? . . . [W]e hold they did not. Since they did not, there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment." *Id*.

[37] 468 U.S. 705 (1984).

private dwelling or in a place "not open to visual surveillance."[38] These holdings, though substantial, spoke only of government-owned surveillance equipment, failing to envision the future governmental attempts to demand similar tracking information from third party service providers.[39] As cellular technology developed, the government began requesting location information from third parties; however, the government met resistance by third parties hesitant to provide the government with such information for fear of possible liability, even though such fear was unfounded.[40] Congress, cognizant of the rapidly increasing technology and the possible harms to individual privacy, decided to act.[41]

The Electronic Communications Privacy Act of 1986 is the seminal legislation outlining electronic surveillance law.[42] Reacting to still-

---

[38] *Id*. at 714. The Court continued:

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.

Id. at 716.

[39] *See id*. at 708 (government owned pager planted pursuant to court order in a can of ether); *see also Knotts*, 460 U.S. at 276 (government owned pager planted during chloroform purchase).

[40] *See* United States v. Miller, 425 U.S. 435, 440 (1976) (individual making a bank deposit had no protectable Forth Amendment interest in bank records).

[41] *See infra* Parts II.A.1-II.A.3 (discussing the various acts within the ECPA).

[42] The main purpose of the ECPA was to "amend[ ] title III of the Omnibus Crime Control and Safe Streets Act of 1968—the Federal wiretap law—to protect against unauthorized interception of electronic communications." S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555. The creators of the ECPA gave specific credence to Justice Brandies' prediction in *Olmstead v. United States*:

> Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. . . . Can it be that the Constitution affords no protection against such invasions of individual security?

277 U.S. 438, 474 (1928).

However, the ECPA had vast, perhaps unintended, consequences on technology law as it became the main vehicle through which the government requested authorization to utilize cell site information for tracking purposes. *See generally* Treglia, *Trailing Cell Phones*, *supra* note 4 (discussing the improbability that Congress thought of the capabilities of cell phone technology when it required information secured from mobile tracking devices to be obtained with a search warrant).

increasing technology including "large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing," Congress intended Title I of the ECPA to address the interception of wire, electronic, and oral communications.[43] Title II of the ECPA addresses government access to "stored wire and electronic communications and transactional records,"[44] while Title III of the ECPA addresses "pen registers and trap and trace devices."[45] The following sections discuss the Titles of the ECPA in greater detail.[46]

1. Title I: The Amended Wiretap Act

Title I of the ECPA amended the 1968 federal wiretap statute[47] to include electronic communications.[48] Title I also represents the highest

---

[43] S. REP. NO. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. at 3556; *see also infra* Part II.B.1 (examining the Wiretap Act, which deals with the information actually communicated by users over various electronic communications devises).

[44] S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. at 3557; *see also infra* Part II.B.2 (discussing the SCA, which deals with communication information stored by various third party service providers and invents the specific and articulable facts standard of proof).

[45] S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. at 3557; *see also infra* Part II.B.3 (discussing the Pen/Trap Statute, dealing with non-content information transmitted at the beginning and end of a call).

[46] *See infra* Parts II.B.1-II.B.3.

[47] Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as 18 U.S.C. §§ 2510-2522 (2000)) ("The Wiretap Act"). The Omnibus Crime Control & Safe Streets Act created what have been deemed "super-warrant" requirements for wiretaps and bugs. *See* SDTX#1, 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005) (describing the highest level of governmental proof as a super warrant showing); *see also* 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) (describing the requirement of super warrant showing in order to obtain the contents of communications in transit).

The need for congressional protection of private conversation became apparent after the Court first applied Fourth Amendment protection to government interception of a telephone conversation in *Katz v. United States*, 389 U.S. 347 (1967). Only six months earlier, the Court had also extended Fourth Amendment protection to electronic eavesdropping in *Berger v. New York*, 388 U.S. 41 (1967). The congressional response to the two Supreme Court decisions was the Wiretap Act. *See* S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. at 3557.

[48] 18 U.S.C. § 2510 (2000). In the mid 1980s, Congress felt it necessary to amend the Wiretap Act in order "to bring it in line with technological developments and changes in the structure of the telecommunications industry." S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. at 3557. Thus, in addition to wire and oral communication, Congress required super warrant showings in order to "intercept" the "contents" of "electronic communication." 18 U.S.C. § 2510. These terms are defined as:

> (4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device. . . .

level of protection afforded to cellular communications under the Fourth Amendment.[49] Further, and more importantly, Title I excluded from the meaning of electronic communications, "any communication from a

---

> (8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .
> (12) "electronic communication" means 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.

Id.

[49] Title I of the ECPA imposed tough restrictions on governmental ability to intercept phone conversations. In fact, the Act requires that:

> (3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that—
>
> > (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter;
> > (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
> > (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
> > (d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

18 U.S.C. § 2518.

Thus, a wiretap may only be ordered if it "is authorized only for specific crimes, for a limited duration, as a last resort, with minimized interception of innocent conversations, notice to targets, and extensive judicial oversight." SDTX#1, 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005).

tracking device."[50] The section of Title I dedicated to mobile tracking devices[51] allows courts empowered with the ability to issue warrants or orders for the installation of tracking devices within their individual jurisdictions to monitor tracking devices that may move across district lines.[52] A tracking device is defined as "an electronic or mechanical device which permits the tracking or the movement of a person or object."[53]

2. Title II: The Stored Communications Act

Title II of the ECPA, known as the SCA, authorizes government access to stored communications and transaction records held by third party mobile service providers.[54] The obtainable information is broken

---

[50] 18 U.S.C. § 2510(12)(C). As discussed *infra* in Parts II.C.1-II.C.2, and Part III, this distinction has served as a major basis for the majority position's adherence to the probable cause standard.

[51] 18 U.S.C. § 3117 (2000).

[52] *Id.* Although not expressly stated, courts have construed the language of § 3117 very narrowly, giving it no effect on the legal standard necessary to obtain an order authorizing the use of a tracking device. *See SDTX#1*, 396 F. Supp. 2d at 751-52 ("The purpose of [§ 3117] was narrow: to authorize monitoring of tracking devices which may move across district lines. . . . A Rule 41 probable cause warrant was (and is) the standard procedure for authorizing the installation and use of mobile tracking devices."); *see also* United States v. Mixon, 717 F. Supp. 1169 (E.D. La. 1989) (requiring a probable cause warrant before a government could install a beeper on a plane for tracking purposes); United States v. Karo, 468 U.S. 705, 720 (1984) (holding that a Rule 41 warrant was necessary in order to monitor a beeper in a private residence and failure to obtain one violated the Fourth Amendment).

Effective December 1, 2006, Rule 41 was amended, giving federal magistrate judges the authority to issue warrants to install tracking devices within their respective districts. The changes included giving the term "tracking device" the same meaning as that in Title I of the ECPA, allowing magistrate judges to issue warrants authorizing the tracking of a "person or property located within the district" or "outside the district" commanding the magistrate judges to issue such warrants if an affidavit or other information provided by a government official illustrates that there is "probable cause to search for and seize a person or property or to install and use a tracking device," and stating that the tracking device may not be used for more than forty-five days unless the court feels it necessary to grant extensions not to exceed forty-five days each.

[53] 18 U.S.C. § 3117(b) (2000).

[54] 18 U.S.C. §§ 2703-2712 (2000). Section 2703 lays out various methods of obtaining stored communications and transactional records. *Id.* Specifically, § 2703(c)(1)(A)-(D) states:

> (c) **Records concerning electronic communication service or remote computing service**.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with

into three categories: (1) contents of wire or electronic communications in electronic storage;[55] (2) contents of wire or electronic communications in a remote computing service;[56] and (3) records concerning electronic communication service or remote computing service.[57] In 1994, the government's burden for obtaining the third category of information, involving actual customer records, was raised to the standard of "specific and articulable facts."[58] Prior to 2005, it was common for

---

> jurisdiction over the offense under investigation or equivalent State warrant;
> (B) obtains a court order for such disclosure under subsection (d) of this section;
> (C) has the consent of the subscriber or customer to such disclosure;
> (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title).

[55] *Id*. § 2703(a). Generally, this information is only obtainable pursuant to a warrant obtained under Rule 41 upon a showing of probable cause, or with notice to the customer. *Id*.

[56] 18 U.S.C. § 2703(b). Similar to information in electronic storage, this information is only obtainable pursuant to Rule 41 upon a showing of probable cause, or with notice to the customer; however, both electronic storage information and remote computing service information may be obtained pursuant to a § 2703(d) order (discussed *infra* note 59 and accompanying text), the former only when information has been in the storage system for more than one hundred and eighty days. *Id*.

[57] *Id*. § 2703(c). These records are available either by warrant pursuant to Rule 41, the consent of the customer, or a § 2703(d) order based on specific and articulable facts (discussed *infra* at note 59 and accompanying text).

[58] Pub. L. No. 103-414, 108 Stat. 4292 (1994). The original standard for obtaining customer records was a showing that there was "reason to believe . . . the records or other information sought, are relevant to a legitimate law enforcement inquiry." *SDTX#1*, 396 F. Supp. 2d at 752 n.7 (quoting Pub. L. No. 99-508, 100 Stat. 1861 (1986)). In 1994, Congress passed the Communications Assistance for Law Enforcement Act, commonly known as CALEA. 47 U.S.C. §§ 1001-1010 (2000). The house report on CALEA stated:

> In the eight years since the enactment of ECPA, society's patterns of using electronic communications technology have changed dramatically. Millions of people now have electronic mail addresses. Business, nonprofit organizations and political groups conduct their work over the Internet. Individuals maintain a wide range of relationships on-line. Transactional records documenting these activities and associations are generated by service providers. For those who increasingly use these services, this transactional data reveals a great deal about their private lives, all of it compiled in one place. . . . Therefore, [CALEA] includes provisions . . . that add protections to the exercise of the government's current surveillance authority.

H.R. REP. NO. 103-827(I), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3897.

prosecutors to obtain orders to secure some forms of real time cell site information utilizing the specific and articulable facts standard illustrated in the SCA.[59] Beginning in 2005, however, many district courts began to require a showing of probable cause pursuant to Federal Rule of Criminal Procedure 41 ("Rule 41").[60]

3. Title III: The Pen/Trap Statute

Title III of the ECPA concerns pen registers and trap and trace devices.[61] A "pen register" is a device installed within a court's

---

[59] Treglia, *Trailing Cell Phones, supra* note 4, at 2-3. Treglia discusses how it was commonplace for prosecutors to gain various forms of real time information pursuant to § 2703(d) orders, which gain their name from § 2703(d). Section 2703(d) states:

> (d) **Requirements for court order**.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(emphasis added).

Treglia adds that prosecutors, and most courts, viewed the § 2703(d) order as a sort of catch-all category for information that did not fit into the category requiring super warrant showings or the categories of information for which a court subpoena is sufficient. Treglia, *Trailing Cell Phones*, *supra* note 4, at 3; *see also* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH 65, 79 (1997) ("To obtain it in real-time, law enforcement agencies have been using court orders issued under 18 U.S.C. § 2703(d). In 1994, three of the four manufacturers of cellular switches had developed the software capability to deliver location information to law enforcement immediately upon call completion.").

[60] *See infra* Parts II.C.1, III.A (discussing the various district court decisions adhering to the majority view).

[61] 18 U.S.C. §§ 3121-3127 (2000).

> (3) the term "pen register" means 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, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

jurisdiction for the purpose of recording all phone numbers dialed by a single phone; a "trap and trace device" is a device installed within a court's geographical jurisdiction for the purpose of recording all phone numbers received by a single phone.[62] A court is *required* to enter an ex parte order allowing the installation of a pen register or trap and trace device anywhere in the nation if the court determines that the government attorney has "certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[63] Finally, in 2001, the USA PATRIOT Act expanded the definition of a pen register to include addressing information of electronic communications.[64]

> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

Id. § 3127(3)-(4).

[62] *Id*. § 3127; *see SDTX#1*, 396 F. Supp. 2d at 752; *see also* United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1967) ("A pen register is 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. It does not overhear oral communications and does not indicate whether calls are actually completed.").

The Court, in *Smith v. Maryland*, held that people do not have a reasonable expectation of privacy in telephone numbers they dial, therefore, failing the first prong of the *Katz* test. 442 U.S. 735, 742 (1979). The Court reasoned:

> All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

Id.

[63] 18 U.S.C. § 3121(a)(1). This is the lowest standard a government official must meet in order to gain cell site information from a third party service provider. *See* Treglia, *Challenge of Tracking*, *supra* note 2, at 2 (discussing the four levels of proof required for various cell site information).

[64] Pub. L. No. 107-56, § 216, 115 Stat. 272, 288 (2001). Titled, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act," the USA PATRIOT Act, amended 18 U.S.C. § 3121(c), now reads:

> (c) **Limitation**.—A government agency authorized to install and use a pen register *or trap and trace device* under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, *routing, addressing, and signaling information* utilized in *the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.*

C. The Current District Split

The ECPA thus sets out four broad, distinguishable categories of legal process required for government officials to obtain judicial permission to gather various types of cell site information from third party service providers:[65] (1) To intercept conversation content, the government must meet super warrant requirements;[66] (2) to obtain cell site information from tracking devices, the government must show probable cause pursuant to Rule 41;[67] (3) to obtain customer records, the government must show specific and articulable facts pursuant to 18 U.S.C. § 2703(d);[68] and (4) to obtain information from a pen register or trap and trace device, the government must illustrate that such material is relevant to an ongoing criminal investigation.[69] Against this statutory framework, beginning in 2005, many federal district courts attempted to determine what level of process was required in order to obtain prospective, real time cell site information from third party cellular service providers.[70]

1. The Majority Position: Probable Cause Showing

The Eastern District of New York was the first district to examine the question.[71] There, the government requested disclosure of real time cell site information by way of a dual order, the first allowing the government to obtain the information and the second demanding the service provider to turn it over.[72] The court, after examining whether a cellular phone was better classified as a tracking device or a wire or electronic communication, held that the government was required to

---

Id. § 3121(c) (emphasis added to illustrate changes enacted pursuant to the USA PATRIOT Act).

65 *See* Treglia, *Challenge of Tracking*, *supra* note 2, at 2-3 (discussing the four levels of proof); *see also supra* Part II.B.

66 *See supra* Part II.B.1.

67 *See supra* Part II.B.2.

68 *See supra* Part II.B.2.

69 *See supra* Part II.B.3.

70 *See infra* Parts II.C.1-II.C.2.

71 *In re* an Application of the U.S.A. for an Order (1) Authorizing the Use of a Pen Register and Trap and Trace Device and (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005) [hereinafter EDNY#1].

72 *Id*. at 563. The government sought information by way of a pen register and trap/trace device. *Id*. The Magistrate Judge initially expressed doubt about whether he could order such information and requested the government to provide authority supporting its request. The government declined. *Id*.

make a probable cause showing in order to obtain real time cell site information.[73]

Federal Magistrate Judge Smith in the Southern district of Texas soon followed suit,[74] holding that the tracking device category is the exclusive fit for prospective, real time cell site information.[75] In making

---

[73] *Id*. at 564-65. Specifically, the court stated that the

> only [section of the ECPA] that appears arguably to permit the disclosure of cell site location information is the language permitting the disclosure of "the contents of a wire or electronic communication" upon an offer of "specific and articulable facts showing that there are reasonable grounds to believe that [such information is] relevant and material to an ongoing criminal investigation."

Id. at 563 (citing 18 U.S.C. § 2703(d)).

However, the court found that the information the government requested would turn the targeted mobile phone into a tracking device, or "'an electronic or mechanical device which permits the tracking of movement of a person or object.'" *Id*. at 564 (citing 18 U.S.C. § 3117(b)). The court likened the requested tracking ability to physical surveillance of a person, concluding that both "revea[l] that person's location at a given time." *Id*. Further, the court left open the possibility that the ECPA, by its language, may allow magistrate judges the ability to give permission for the government to obtain cell site information. *Id*. at 565. However, to allow such a reading of the ECPA would be contrary to congressional intent because it would allow a very low standard of proof for a great intrusion on personal privacy. *Id*. Finally, the magistrate judge admitted to having granted such requests in the past, even as recently as four months earlier, without questioning the legal basis for having done so. *Id*. at 566. Quoting Justice Frankfurter, the judge concluded: "'Wisdom too often never comes, and so one ought not to reject it merely because it comes late.'" *Id*. (citing Henslee v. Union Planters Nat'l Bank & Trust Co., 335 U.S. 595, 600 (1949) (Frankfurter, J., dissenting)).

[74] SDTX#1, 396 F. Supp. 2d 747 (S.D. Tex. 2005).

[75] *Id*. at 754 ("[T]he only permissible inference is that Congress intended 'tracking device' to have the broader meaning."). After a very detailed analysis of cell phone technology and the ECPA, the court examined the breadth of the ECPA definition of "tracking device." *Id*. at 750-57. The court stated that a device was covered by the definition "even though it may not have been intended or designed to track movement; it is enough if the device merely 'permits' tracking." *Id*. at 753. Congress may have been anticipating advancements in tracking technology by giving such an expansive definition of a tracking device. *Id*. The court continued, "even traditional tracking devices such as beepers on vehicles are now monitored via radio signals using the very same cell phone towers used to transmit cell site data. Given this convergence in technology, the distinction between cell site data and information gathered by a tracking device has practically vanished." *Id*. at 754.

The court then described how law enforcement converts a cell phone into a tracking device when it uses cell site information to create a virtual map of a suspect's whereabouts. *Id*. Moreover, the court discussed how "[l]ocation based services" will be a large part of new cell phone features, spurred by possible market advantages. *Id*.; *see also* David J. Phillips, *Beyond Privacy: Confronting Locational Surveillance in Wireless Communications*, COMM. L. & POL'Y, Winter 2003, at 11-13 (discussing the rise of location based services and the market forces driving this phenomenon). The court concluded, "This inexorable

its determination, the court cited Fourth Amendment concerns, noting that phones may be monitored in a person's home and without her knowledge.[76]

The federal districts of the District of Columbia,[77] Maryland,[78] Northern Indiana,[79] Eastern Wisconsin,[80] Western New York,[81] and Southern New York[82] followed the same logic, each holding that the

---

combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year." *SDTX#1*, 396 F. Supp. 2d at 755.

After determining that cell site information was correctly categorized under information sought by a tracking device, the court dismissed the government's dual theory, which combined provisions of the SCA and the Pen/Trap Statute (discussed *infra* at Part II.C.2), stating: "Far from the silent synergy of disparate statutes now posited by the government, the FBI director in 1994 was insisting that the Pen/Trap Statute has 'nothing to do with' the SCA, and that transactional information 'is exclusively dealt with in chapter 121 of Title 18,' *i.e.*, the SCA." *Id.* at 764 ("'The FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past.'" (quoting H.R. REP. NO. 103-827(I), at 24 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3504)).

[76] *SDTX#1*, 396 F. Supp. 2d at 765. The court concluded by stating that prudential interests required a judgment in favor of privacy rights, absent any congressional authorization in favor of law enforcement. *Id.*

[77] The D.C. District visited this question three times. *See In re* the Application of U.S.A. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134 (D.D.C. 2006) [hereinafter DDC#3]; *In re* the Application of U.S.A. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 132 (D.D.C. 2005) [hereinafter DDC#2]; *In re* the Applications of U.S.A. for Orders Authorizing Disclosure of Cell Site Info., Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531 (D.D.C. Oct. 26, 2005) [hereinafter DDC#1].

[78] The Maryland District visited the question twice: *In re* the Application of U.S.A. for orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices on Tel. Numbers, 416 F. Supp. 2d 390 (D. Md. 2006) [hereinafter DMD#2]; and *In re* the Application of U.S.A. for an Order Authorizing Installation and Use of a Pen Register and a Caller Identification Sys. On Tel. Numbers, 402 F. Supp. 2d 597 (D. Md. 2005) [hereinafter DMD#1].

[79] *In re* the Application of the U.S.A. for an Order (1) Authorizing the Installation and Use of a Pen register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location-Based Services, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006) [hereinafter NDIND].

[80] *In re* the Application of U.S.A. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947 (E.D. Wis. 2006) [hereinafter EDWIS#1].

[81] *In re* the Application of U.S.A. for an Order Authorizing Installation and Use of a Pen Register, 415 F. Supp. 2d 211 (W.D.N.Y. 2006) [hereinafter WDNY].

[82] *In re* the Application of U.S.A. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 CRIM. MISC. 01, 2006 WL 468300 (S.D.N.Y. Feb. 28, 2006) [hereinafter SDNY#2]. It is important to note here that this is Federal Magistrate Judge Peck's opinion. *Id.* Like the Southern district of Texas, the Southern District of New York is split as to what proof is required for prospective cell site information. *See In re* the Application of U.S.A. for an Order (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other

present state of the law did not allow the government to obtain prospective, real time cell site information from a court order based on any showing lower than probable cause.[83] While the majority of courts

---

Info., 433 F. Supp. 2d 804 (S.D. Tex. 2006) [hereinafter SDTX#2] (allowing limited prospective cell site information under the hybrid theory); *see also In re* the Application of U.S.A. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) [hereinafter SDNY#1] (same).

[83] In its first decision, the D.C. District found that cell site information may not be disclosed pursuant to the SCA, the Pen/Trap Statute, or both. *DDC#1*, 2005 WL 3658531, at *1. Further, the court held that no other magistrate judge within the district would accept any level of proof below probable cause for such orders. *Id*.

In its second decision, the D.C. District once again demanded a showing of probable cause under Rule 41, this time in reaction to the government's attempt to acquire real time cell site information by a showing of "probable cause to believe that the requested prospective cell site information is relevant and material to an ongoing criminal investigation." *DDC*#2, 407 F. Supp. 2d at 133. This new hybrid theory, a combination of the pen/trap standard and the probable cause standard was held to be merely an ineffective attempt to overcome the Texas and New York decisions. *Id*. The court stated:

> 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. . . . Obviously, the statement that there is probable cause to believe that the information is relevant and material to an ongoing criminal investigation is tautological.

Id.

The third D.C. decision denied yet another attempt by the government to utilize the Pen/Trap Statute in combination with CALEA. *DDC*#3, 407 F. Supp. 2d at 137. The government attempted to re-interpret 47 U.S.C. § 1002 (CALEA), which disallows "information acquired *solely* pursuant to the authority for pen registers and trap and trace devices . . . that may disclose the physical location of the subscriber." *Id*. (citing 47 U.S.C. § 1002 (2000)) (emphasis added). The government theorized that because its request combined the Pen/Trap Statute with the specific and articulable facts phrasing of the SCA, it was not attempting to acquire the location of a subscriber *solely* pursuant to the Pen/Trap Statute. *Id*. The court disagreed stating:

> It is inconceivable to me that the Congress that precluded the use of the Pen Register statute to secure in 1994 "transactional data" or what [former FBI Director] Freeh called "call up information" nevertheless intended to permit the government to use that same statute, whether by itself or combined with some other means, to secure the infinitely more intrusive information about the location of a cell phone every minute of every day that the cell phone was on. I cannot predicate such a counter-intuitive conclusion on the single word "solely."

Id. at 140 (quoting 47 U.S.C. § 1002).

The Maryland District, in its first decision, also denied government use of the hybrid theory. *DMD#1*, 402 F. Supp. 2d at 605. The court joined the other districts in holding that "cell site information is not a record concerning electronic communication service or remote computing service and is therefore not covered by" the SCA. *Id*. at 602. Using stronger language than the courts before it, the Maryland District stated:

> The court will not enter an order authorizing disclosure of real time cell site information under authority other than Rule 41, nor upon a

> showing of less than probable cause. To the extent the government seeks to act without a warrant, the government acts at its peril, as it may not monitor an electronic tracking device in a private place without a warrant.

Id. at 605.

In its second decision, the Maryland District again disallowed the government's hybrid theory stating:

> even if the court concluded Congress intended the Pen/Trap Statute to authorize disclosure of cell site information when combined with other authority, that authority is *not* the SCA. First, the SCA simply is not and never was intended to be a statute that authorizes prospective surveillance. The structure of the SCA shows that the statute does not contemplate orders for prospective information. . . . The bottom line is that the hybrid theory . . . advocated by the government leaves the court with authority that is at best murky and, at worst, illusory. Where prospective surveillance of a person's location is concerned, the court cannot base an order on such shaky authority. Only Congress may authorize courts to order disclosure of prospective cell site information on a showing of less than probable cause, and it is not clear that Congress has done so.

DMD#2, 416 F. Supp. 2d at 395-97; *see also* Caryn Tamber, *Probable Cause Still Rules for Cell Location Data*, KAN. CITY DAILY REC., Aug. 7, 2006 ("A Maryland judge's denial last month of a government request to track a fugitive via his cell phone signals is the latest skirmish in a growing battle over when officials may use the practice.").

The Northern District of Indiana joined the other districts stating:

> (1) the Government cannot rely on the Pen Register Statute to obtain cell site location information; and (2) converging the Pen Register Statute with the SCA in an attempt to circumvent the exception in the CALEA is contrary to Congress' intent to protect cell site location information from utilization as a tracking tool absent probable cause under the Fourth Amendment. The legal rationale supporting these conclusions can be found in numerous opinions from other jurisdictions.

NDIND, 2006 WL 1876847, at *4.

The Eastern District of Wisconsin, relying heavily on legislative history, also rejected the government's hybrid theory. *EDWIS#1*, 412 F. Supp. 2d at 958. Relying on former FBI Director Freeh's congressional testimony in support of the CALEA, the court stated:

> Director Freeh assured Congress that the legislation about which he was testifying and urging Congress to pass had nothing to do with, and did not relate to, the SCA, to wit, 18 U.S.C. § 2701, *et seq*. In the face of such testimony, it makes no sense to me that, by the use of the word "solely" in 47 U.S.C. § 1002(a)(2), Congress was in some back-handed fashion intending to allow the SCA to be used in conjunction with the Pen/Trap Statute to obtain the very information that Director Freeh assured Congress he was not seeking the authority to obtain under the proposed legislation.

Id. at 958.

The Western District of New York, although seemingly more sympathetic to some of the government's arguments, also rejected the dual theory and concluded that a probable cause showing was necessary for prospective, real time cell site information. *WDNY*, 415 F. Supp. 2d at 219. The court felt it would be outside the scope of judicial power to piece together statutes, some created fifteen years apart from each other, in order "allow law

required probable cause, a minority allowed at least limited access to real time cell site information.[84]

2. The Minority Position: Specific and Articulable Facts

The first opinion adhering to the minority position arose in the Southern District of New York.[85] There, instead of seeking all available cell site information, including information transmitted during the registration process, the government sought only real time information tied to calls made and received by the telephone user.[86] Further, the government sought only information from one cell site at a time, disallowing real time triangulation and greatly reducing the specificity with which the government could pinpoint a user's location.[87] Finally,

---

enforcement to use a pen register device to obtain real time cell location data, at least on anything less than a showing of probable cause." *Id*. at 214. The court further admitted, that "[t]he government's concerns over the 'ambiguity of the statutes' are well founded, but it is the Congress and not the Department of Justice who is empowered to respond to those concerns." *Id*. at 219.

Finally, Magistrate Judge Peck in the Southern District of New York joined the majority position, by departing from the hybrid theory allowed by Magistrate Judge Gorenstein in the same district. *SDNY#2*, 2006 WL 468300, at *2. Magistrate Judge Peck based his decision on the privacy interest effected by the government's request, stating:

> The Court also notes that while the Government's request for cell site location information in this District has been limited to general tower location (not triangulation information that can more precisely give the cell phone's location) and only for the origination and termination of calls, the Government's statutory interpretation would allow it to obtain triangulation location information for the entire duration of the call and, indeed, for all times the cell phone is on, even when no call is in progress.

Id.

[84] *See infra* Part II.C.2 (discussing the district court decisions adhering to the hybrid theory and granting real time cell site information based on a showing of specific and articulable facts.).

[85] SDNY#1, 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

[86] *Id*. at 438. Notably, this information, unlike registration information, is transmitted with full knowledge of the phone user. *Id*. at 449 ("[T]he individual has chosen to carry a device and to permit transmission of its information to a third party, the carrier."). The registration process occurs every seven seconds or when signal strength drops below a chosen threshold, automatically, and without the users knowledge. *See* Farley, *supra* note 23, at http://www.privateline.com/Cellbasics/Cellbasics03.html (discussing the process of registration and the purposes behind it.).

[87] *SDNY#1*, 405 F. Supp. 2d at 438 ("Thus, no data is provided that could be 'triangulated' to permit precise location of the cell phone user."). The court further stated that this information could not be used to create a "virtual map" of a mobile phone user's location. *Id*. at 449. Specifically:

> The information does not pinpoint a user's location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more

the government did not request the information directly, asking that it be "transmitted from the provider digitally to a computer maintained by the [g]overnment."[88] For the first time, the Southern District of New York accepted the government's dual authority position, combining the Pen/Trap Statute[89] with the SCA,[90] by way of CALEA.[91] The Western

---

> miles apart in rural areas and may be up to a half-mile or more apart even in urban areas.

Id.

88 *Id*. at 438. The government would then use software to create a spreadsheet of the information obtained from the third party service provider. *Id*.

89 18 U.S.C. §§ 3121-3127; *see also supra* Part II.B.3 (discussing the Pen/Trap Statute, dealing with non-content information transmitted at the beginning and end of a call).

90 18 U.S.C. § 2703; *see also supra* Part II.B.2 (discussing the SCA, which deals with communication information stored by various third party service providers and invents the specific and articulable facts standard of proof).

91 47 U.S.C. § 1002 (2000). The court determined that, "construing the pen register definition as covering the capture of cell site data is the only way to make sense of a separate statute: 47 U.S.C. § 1002." *SDNY#1,* 405 F. Supp. 2d at 439. Referring to CALEA, the court broke with the previous decisions on the intent of the word "solely," and gave it a strict textual meaning. *Id*. at 442.

> While we have extracted some semantic content out of the word "solely," it has hardly been a satisfying exercise inasmuch as we are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination of the Pen Register Statute with some other unspecified mechanism.

Id. The court felt that to hold otherwise would be to "ignore the plain dictate of" the Pen/Trap Statute by assuming another provision was intended to intercept an individual's whereabouts. *Id*. at 442-43. The other option, the court reasoned, was to ignore the plain language of CALEA by ignoring Congress's choice to include the word "solely." *Id*. at 443 (citing 47 U.S.C. 1002); *see also* Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997) ("The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole."). *But see* EDWIS#1, 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006) ("[I]t makes no sense to me that, by the use of the word "solely" in 47 U.S.C. § 1002(a)(2), Congress was in some back-handed fashion intending to allow the SCA to be used in conjunction with the Pen/Trap Statute.").

After determining that some mechanism was intended to be used in combination with the Pen/Trap Statute, the court found that the SCA was "the most obvious candidate." *SDNY#1*, 405 F. Supp. 2d at 448. The court reasoned that the absence of procedural steps for transmitting cell site information was easily explained by the fact that the Pen/Trap Statute, which requires many procedures (*see* 18 U.S.C. § 3121(c)), was intended by Congress as the "proper 'device' to obtain cell-site information." *Id*. at 449. The court concluded by again mentioning the very narrow scope of the holding:

> Because the Court cannot know how that technology may change, it intends to identify specifically, in any future orders authorizing the provision of cell site information, the character of the information that may be provided by a carrier. Specifically, any such Order will make clear that it contemplates the production only of: (1) information regarding cell site location that consists of the tower receiving

District of Louisiana soon joined the minority position, accepting the dual authority position and attaching the same limitations as the Southern District of New York.[92]

Next, the Southern District of West Virginia allowed the government to obtain real time tracking information based on specific and articulable facts; however, the court rejected the dual authority position, instead relying on the fact that a fugitive was using another person's mobile phone and was not considered a "subscriber" under CALEA.[93] Because the user of the mobile phone was not the subscriber, the Southern District of West Virginia allowed the government "the authority to obtain Cell Site Location Information, without geographic limitation within the United States," the most expansive amount of real time information ever allowed by a district court based on a showing of specific and articulable facts.[94]

> transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and (3) information that is transmitted from the provider to the Government. If the Government seeks to obtain other information, it should provide additional briefing on why such information is permissible under the relevant authorities.

Id. at 450.

The government attempted to re-interpret 47 U.S.C. § 1002, which disallows "information acquired *solely* pursuant to the authority for pen registers and trap and trace devices . . . that may disclose the physical location of the subscriber," by combining the Pen/Trap authorization for devices that used to obtain cell-site information, with the SCA's clear and articulable facts burden. *Id*. (emphasis added); *see also SDNY#1*, 405 F. Supp. 2d at 438.

92 WDLA, 411 F. Supp. 2d 678, 680 (W.D. La. 2006) ("Because I agree with Magistrate Judge Gorenstein's analysis of the relevant statutory framework, I adopt his detailed analysis and will allow the Government to obtain the same information *subject to the same limitations*."). Citing the conclusion that mobile phone users "know that third party service providers are aware of their general location viv-a-vis the nearest tower, at the beginning of, during and at the end of each call," the court concluded that when the government requests only single tower information, accessed when a user makes or receives a call, and the cell site information is transmitted from the service provider to the government, "no Fourth Amendment concerns are implicated" and a showing of specific and articulable facts will suffice. *Id*. at 681-82.

93 SDWVA, 415 F. Supp. 2d 663, 666 (S.D. W. Va. 2006). Because CALEA refers to the "subscriber" in limiting the authority to identify a person's whereabouts, the court felt that a person merely using someone else's mobile phone was not entitled to that protection. *Id*. at 666 ("[T]he person sought by the Marshals Service is *not* the *subscriber*. The *user* of a cellphone who is *not* the subscriber has no protection pursuant to 47 U.S.C. § 1002(a)(1).").

94 *Id*. It is interesting to note that the court gave a great amount of credence to the word "subscriber" in 47 U.S.C. § 1002, while at the same time rejecting the government's dual authority position based on the reasoning in previous decisions. *Id*. at 665 (after reviewing

Soon thereafter, adhering to many of the safeguards present in the case before the Southern District of New York,[95] Magistrate Judge Rosenthal in the Southern District of Texas allowed the government to obtain real time cell site information "at the origin and termination of calls and, if reasonably available, during the progress of a call that is not initiated by the government itself."[96]

Finally, District Judge Kaplan, yet another voice ruling in the Southern District of New York, held that obtaining prospective cell site information from a single cell phone was authorized by the dual authority position, "at least where . . . the government does not seek triangulation information or location information other than that transmitted at the beginning and end of particular calls."[97] Interestingly, the court noted the apparent tension between the congressional intent for enacting the SCA, Pen/Trap Statute, and CALEA respectively, and the authorization the plain language of the acts allow when used together.[98]

---

the previous decisions on point, the court stated, "The undersigned is unpersuaded by the government's argument that Chapters 206 and 121, considered together, permit a court to authorize use of a pen register and trap and trace device in order to locate a *subscriber* using a cell phone in a geographical area, despite the provisions of 47 U.S.C. § 1002(a)(1).").

The irony is that most of the previous decisions focused on the word "solely" and how it was meaningless and contrary to congressional intent. *See supra* note 83 and accompanying text. Thus, while giving great credence the word "subscriber", as opposed to "user," the court overlooked the word "solely" as meaningless (a word found in the very paragraph of the chosen word "subscriber") in order to allow sweeping government surveillance based on a showing less than probable cause. *See* 47 U.S.C. § 1002 (a)(2) ("except that, with regard to information acquired *solely* pursuant to the authority for pen registers . . . such call information shall not include any information that may disclose the physical location of the *subscriber*") (emphasis added).

95 *SDNY#1*, 405 F. Supp. 2d at 438 (allowing prospective, real time cell site information based only on calls made or received by the mobile phone user, from a single tower, and supplied indirectly to the government).

96 SDTX#2, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006). In a simple analysis of the preceding cases, Judge Rosenthal addressed the competing district views and likened the facts to those in the Southern District of New York case. *Id*. at 805-06. Concluding that the government sought information with less privacy implications than in previous decisions which rejected the hybrid theory, the court granted the government's application based on analogy to similar facts. *Id*. at 806.

97 SDNY#3, No. 06 CRIM. MISC. 01, 2006 WL 3016316, at *9 (S.D.N.Y. Oct. 23, 2006). The court used a strict textual analysis, stating "[c]ourts 'do not resort to legislative history to cloud a statutory text that is clear,' even in the face of 'contrary indications in the statute's legislative history.'" *Id*. at *5 (quoting Co. of Suffolk v. First Am. Real Estate Solutions, 261 F.3d 179, 190 (2d Cir. 2001) (quoting Ratzlaf v. United States, 510 U.S. 135, 147-48 (1994))).

98 *Id*. at *1.

> Although there is little indication that Congress actually intended that the Pen Register Statute and the Stored Communications Act could be combined to authorize the disclosure of prospective cell site information, the language of the two statutes, when read together,

Nevertheless, the court felt bound to follow the clear language of the statutes and allowed the government to obtain the information.[99]

While a number of courts have made strong arguments for both positions based on difficult statutory interpretations, the end result is a conflicting jurisprudence that lends itself to prosecutorial misuse.[100]

III. ANALYSIS OF JURISPRUDENTIAL INTERPRETATIONS OF ELECTRONIC SURVEILLANCE STATUTES AS APPLIED TO GOVERNMENT REQUESTS FOR REAL TIME CELL SITE INFORMATION

> *"Until they become conscious they will never rebel, and until after they have rebelled they cannot become conscious."*[101]

Like Orwell's Proles, it took decisions by various magistrate judges to change the common practice of granting government access to cell site information absent the correct showing.[102] However, the judges were met with prosecutorial resistance.[103] The background surrounding the use of prospective cell site information illustrates an evolution of thought by federal prosecutors.[104] Prior to the recent decision of many districts to reevaluate the practice of routinely allowing prospective cell site information by way of the § 2703(d) order, prosecutors realized what powerful tracking tools cellular telephones could be and began to request any and all information that could feasibly aid them in an investigation.[105] However, as evidenced by the majority position, once prosecutors sought to track suspects based on triangulation information

---

> clearly authorizes such disclosure. The Court is bound to follow such clear statutory language. Congress nevertheless may wish to consider whether this result is consistent with its intention.

Id.

99 *Id*. at *11.

100 *See* Treglia, *Trailing Cell Phones*, *supra* note 4, at 4 (observing that the current split of authority creates the reality that "prosecutors, as they learn which side of the fence which courts sit, will approach those more likely to issue lower proof-level orders")

101 *See* Orwell, *supra* note 1, at 74.

102 *See supra* Parts II.C.1-II.C.2 (discussing the various district court decisions).

103 *See supra* Parts II.C.1-II.C.2 (describing the various attempts by government agents to gain various forms of information including multiple tower triangulation, single tower information, and non-subscriber information).

104 *See supra* Parts II.C.1-II.C.2.

105 *See Who Knows Where You've Been*, *supra* note 33, at 310-11 (discussing the various uses by law enforcement of cellular location information).

transmitted absent any knowledge of the mobile user, courts overlooked clear textual analysis in favor of legislative history supporting privacy.[106]

Confronted with the reality that federal judges were hesitant to allow such encroachments upon individual privacy even in the face of statutory text, prosecutors then attempted to gain less intrusive information such as that related from a single tower, from a single phone, or information limited to incoming and outgoing calls.[107] Armed with the very same statutory text as the majority position, but absent the overwhelming privacy interests, districts adhering to the minority position limited review to plain textual analysis and ignored the legislative history relied upon by the majority.[108] Thus, prosecutors have managed to obtain some prospective cell site information without a showing of probable cause based on inconsistent reasoning by various district courts; however, this outcome poses a fundamental question: Does a strict textual analysis resulting in a burden of proof clearly contrary to congressional intent adequately protect the privacy interests of cell phone users, or is a heightened level of proof necessary?[109]

Part III.A of this Note will analyze the hybrid theory, focusing on both the benefits it affords to law enforcement and its failure to give credence to congressional intent.[110] Next, Part III.B will examine the

---

106 *See supra* Part II.C.1 In fact, a reason echoed in many majority decisions overlooked plain language as being the improbable result of congress. *See SDTX#1*, 396 F. Supp. 2d at 764 (overlooking the plain text of the statute and stating, "Far from the silent synergy of disparate statutes now posited by the government, the FBI director in 1994 was insisting that the Pen/Trap Statute has 'nothing to do with' the SCA, and that transactional information 'is exclusively dealt with in chapter 121 of Title 18,' *i.e.*, the SCA."); DDC#3, 407 F. Supp. 2d 134, 140 (D.D.C. 2006) (admitting the plain language of the statute gave some validity to the governments position, but concluding, "I cannot predicate such a counter-intuitive conclusion on the single word 'solely.'").

107 *See supra* Part II.C.2 (discussing the minority position).

108 *See* SDNY#1, 405 F. Supp. 2d 435, 442 (S.D.N.Y. 2005) ("While we have extracted some semantic content out of the word 'solely,' it has hardly been a satisfying exercise inasmuch as we are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination . . . ."); *see also* SDNY#3, No. 06 CRIM. MISC. 01, 2006 WL 3016316, at *1 (S.D.N.Y. Oct. 23, 2006) ("Although there is little indication that Congress actually intended that the Pen Register Statute and the Stored Communications Act could be combined to authorize the disclosure of prospective cell site information, the language of the two statutes, when read together, clearly authorizes such disclosure.").

109 *See infra* Parts III.B-IV (advocating a higher showing of probable cause).

110 *See infra* Part III.A (discussing the hybrid theory and its flaws, namely an encroachment on privacy rights and a complete disregard for congressional intent).

probable cause standard, focusing on its benefits to individual privacy interests and its need for statutory clarification.[111]

A. The Hybrid Theory: A Flawed Attempt

A showing of specific and articulable facts requires that a federal prosecutor must illustrate "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are *relevant and material* to an ongoing criminal investigation."[112] Given the low standard of proof necessary for such a showing, it is not surprising that prosecutors and other government agents have relied on this standard when applying for prospective cell site information.[113] Further, this level of proof is highly beneficial to police and federal agents, as it creates a powerful tool for investigation of suspects based on very little information.[114] This is especially so in situations like kidnapping investigations, where time is of the essence and facts surrounding the crime are few.[115] The districts adhering to the majority position, while recognizing the benefits prospective cell site information could have for police investigations, rejected the specific and articulable facts standard as violative of congressional intent to protect individual privacy rights.[116]

---

111 *See infra* Part III.B (analyzing the probable cause approach and its benefits).

112 18 U.S.C. § 2703(d) (emphasis added); *see also supra* Part II.B.2 (discussing the specific and articulable facts standard). The specific and articulable facts standard is the second lowest standard under the ECPA, only slightly more stringent than the Pen/Trap Statute which requires that the information be relevant to an ongoing criminal investigation. *See* 18 U.S.C. § 3121(a)(1).

113 *See supra* Parts II.C.1-II.C.2 (listing the many cases in which the government has requested prospective cell site information based on a showing of specific and articulable facts).

114 *See Who Knows Where You've Been*, *supra* note 33, at 310-11 (listing many instances in which cell site information has been beneficial to investigators). For instance, the article discusses a Georgia case in which authorities tracked the movements of a man who killed two real estate agents by monitoring his cell phone usage in his car. *Id*. at 310. Another case involved the death of a Vancouver, Washington resident who was shot in her car. *Id*. Her boyfriend denied being near the scene of the crime; however, cell site information placed him within blocks of the scene of the crime. *Id*. Finally, in the prosecution of Scott Peterson for murder of his wife, Laci, the prosecution used Mr. Peterson's cell phone records in order to prove his location. *Id*. Although the evidence was not determinative, it was crucial in impeaching Mr. Peterson's alibi. *Id*. For an analysis of the use of GPS technology as a tool for criminal investigations, see David A. Schumann, *Tracking Evidence with GPS Technology*, WIS. LAW., May 2004, at 9.

115 *See* Treglia, *Challenge of Tracking*, *supra* note 2, at 2 (discussing various cases in which cell phone tracking technology has proved beneficial).

116 *See supra* note 83 and accompanying text (discussing the majority position).

As discussed above, the specific and articulable facts standard is derived from the SCA, which allows the government to obtain "the contents of a wire or electronic communication" upon such a showing.[117] Prospective cell site information seems to fit into the category of "electronic communication" and, presumably, could then be obtained by a showing of specific and articulable facts.[118] However, there is an exception in the "electronic communication" definition, which excludes any "tracking device."[119] Specifically, in order to gain information by way of a tracking device, the government must make a showing of probable cause.[120]

The Eastern District of New York used this exception in holding that a showing of specific and articulable facts was insufficient for prospective cell site information, because it considered "the requested information" to be "useful in the same way that physical surveillance of the telephone user is useful: it reveals that person's location at a given time."[121] The logic further perpetuated the court's holding that authorization to obtain prospective cell site information based solely on

---

[117] 18 U.S.C. § 2703(d). Specifically, the provision states:

> (d) **Requirements for court order**.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A)and shall issue only if the governmental entity offers *specific and articulable facts showing* that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Id.

[118] *Id*. § 2510(12) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . .").

[119] *Id*. (continuing ". . . but does not include. . . . (C) any communication from a tracking device (as defined in section 3117 of this title [18 USCS § 3117])"). 18 U.S.C. § 3117 defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object."

[120] 18 U.S.C. § 3117 states: "If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction."

[121] EDNY#1, 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005). The court continued:

> The fact that the requested order would authorize the disclosure of cell site location information, "if reasonably available, during the progress of a call". . . further suggests that the authorization, if granted, would effectively allow the installation of a tracking device without the showing of probable cause normally required for a warrant.

Id. (citation omitted).

the Pen/Trap statute was improper, notwithstanding the expanded definitions of available material by way of the USA PATRIOT Act, because CALEA expressly forbade acquiring "information that may disclose the physical location of the subscriber,"[122] if such information was acquired "*solely* pursuant to the authority for pen registers and trap and trace devices."[123]

Because the Eastern District of New York focused on CALEA's use of the word "solely," the government was forced to become very creative with its textual analysis, birthing the "hybrid theory" before Magistrate Judge Smith in the Southern District of Texas.[124] Instead of relying solely on the Pen/Trap Statute, the hybrid theory combined sections of the SCA, CALEA, and the Pen/Trap Statute.[125] Judge Smith cogently described the theory:

> The argument proceeds as follows: (1) prospective cell site data falls within the PATRIOT Act's expanded definitions of "pen register" and "trap and trace device" because carriers use cell site data for "routing" calls to and from their proper destination; (2) CALEA amended the law to prevent disclosure of a caller's physical location "solely" pursuant to a pen/trap order, so the government need only have some additional authority

---

122 *Id.* at 565 (quoting CALEA, 47 U.S.C. § 1002(a)(2)(b) (emphasis removed)).

123 *Id.* (quoting CALEA, 47 U.S.C. § 1002(a)(2)(b) (emphasis added)). As discussed *supra* note 64 and accompanying text, the USA PATRIOT Act expanded the amount of information obtainable pursuant to the Pen/Trap Statute. Specifically:

> A government agency authorized to install and use a pen register *or trap and trace device* under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, *routing, addressing, and signaling information* utilized in *the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.*

18 U.S.C. § 3121(c) (emphasis added to illustrate changes enacted pursuant to the USA PATRIOT Act).

The Eastern District of New York noted that although the dialing, routing, and signaling information requested by the government fit within the new definition, the net result would be to allow tracking of individuals pursuant to a standard much lower than probable cause, namely that the information was relevant to an ongoing police investigation. *EDNY#1*, 384 F. Supp. 2d at 565. However, the language of the CALEA forbade such a use, and required that information tending to disclose the physical location of a mobile phone user to be acquired through some other means. *Id.* Thus, the Pen/Trap Statute, by itself, could not be used to acquire prospective cell site information.

124 *See* SDTX#1, 396 F. Supp. 2d 747, 761 (S.D. Tex. 2005) (citations omitted); *see also supra* notes 74-76 and accompanying text (discussing the opinion).

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

> besides the Pen/Trap Statute to gather prospective cell site information; (3) the SCA provides that additional authority, because cell site data is non-content subscriber information obtainable upon a "specific and articulable facts" showing under § 2703(d); and (4) completing the circle, cell site data authorized by a § 2703(d) order may be collected *prospectively* by virtue of the forward-looking procedural features of the Pen/Trap Statute.[126]

On its face, the theory seems quite plausible. If, in fact, a court takes a literal meaning of the word "solely," then information obtainable under the Pen/Trap Statute, but barred by CALEA because it may reveal an individual's location, may be obtained by the addition of the SCA's specific and articulable facts standard. [127] However, although cleverly constructed, the hybrid theory overlooks serious privacy concerns and the legislative intent behind the individual acts.[128]

The first component of the theory, the Pen/Trap Statute, relies upon the USA PATRIOT Act's expanded definitions within that statute.[129] Although the USA PATRIOT Act indeed added "dialing, routing,

---

126 *Id.*

127 *See* SDNY#3, No. 06 CRIM. MISC. 01, 2006 WL 3016316, at *1 (S.D.N.Y. Oct. 23, 2006) ("Although there is little indication that Congress actually intended that the Pen Register Statute and the Stored Communications Act could be combined to authorize the disclosure of prospective cell site information, the language of the two statutes, when read together, clearly authorizes such disclosure."); SDNY#1, 405 F. Supp. 2d 435, 432 (S.D.N.Y. 2005) (stating "[w]hile we have extracted some semantic content out of the word 'solely,' it has hardly been a satisfying exercise inasmuch as we are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination . . . .").

> The use of the word "solely" is significant. "Solely" means "without another'" or "to the exclusion of all else." *See Merriam-Webster's Collegiate Dictionary* (10th ed. 2000), at 1114. If we are told that an act is not done "solely" pursuant to some authority, it can only mean that the act is done pursuant to that authority "*with* [ ] another" authority. *Id.* As a result, the use of the word "solely" in section 1002 necessarily implies that "another" mechanism may be combined—albeit in some unspecified way—with the Pen Register Statute to authorize disclosure of cell site information.

EDWIS#1, 412 F. Supp. 2d 947, 954 (E.D. Wis. 2006).

Magistrate Judge Smith in the Southern District of Texas also recognized "that the text of neither the Pen/Trap Statute nor the SCA mentions such hybrid treatment for cell site data. The government's construction of congressional silence might nevertheless be reasonable, assuming its premises were valid." *SDTX#1*, 396 F. Supp. 2d. at 761.

128 *See infra* notes 129-45 and accompanying text (discussing flaws of the hybrid theory).

129 *See supra* note 64 (discussing the USA PATRIOT Act's changes to the Pen/Trap Statute).

addressing, and signaling information" definitions to the Pen/Trap Statute, the Southern District of Texas focused on the legislative history behind those changes.[130] While admitting that the legislative history of the Act was "abbreviated," the court concluded that the thrust behind the addition was to "update the pen/trap statute to cover Internet traffic" and not to "extend the reach of the Pen/Trap Statute to cell phone tracking."[131] Thus, in the opinion of the majority position, the USA PATRIOT Act never intended utilization of the Pen/Trap Statute for the purposes of obtaining prospective cell site information in any form, let alone in combination with the SCA.[132]

Legislative history also dispels the notion that CALEA was intended to serve as a vehicle by which the government could obtain prospective cell site data absent a showing of probable cause. In fact, the proposal was specifically challenged by many privacy advocates before its passage.[133] Many courts adhering to the majority position pointed to the testimony of then FBI Director Louis Freeh, who came before a joint congressional committee in 1994 to defend CALEA.[134] Mr. Freeh's testimony is extremely revealing when considered against the strict textual adherents of the minority position.[135] First, during his discussion of "call setup information," Mr. Freeh stated that there was "no intent whatsoever, with reference to this term, to acquire anything that could

---

130 *SDTX#1*, 396 F. Supp. 2d at 761-62. The court focused on the house congressional record concerning the USA PATRIOT Act. *Id.*

131 *Id.* at 761. Noting the broad range and importance of the statute, the court concluded, "such an important change in electronic surveillance law would have been noticed by *someone*." *Id.*

132 *Id.* The Southern District of Texas decision also went further, dismissing any implication that the Pen/Trap Statute was ever intended for information obtained without the individual user's knowledge. *Id.* The court reasoned that the original statute, even before the USA PATRIOT Act expansion, was "triggered only when . . . the user attempted to make a call." *Id.* The court found that the expanded definition was "incidental to" this original requirement, and did not dispel it. *Id.* Thus, even if cell phones could conceivably be covered by the Pen/Trap Statute, the only information obtainable would be that transmitted while a user was actively dialing or receiving calls. *Id.*

133 *Id.* at 762-63 (stating that the CALEA "was challenged before passage by some privacy advocates, who worried that the broad definition of call-identifying information would be construed as amending the pen register statute to authorize tracking of cell phone users under that statute's minimal requirements").

134 *See Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Hearings before the Subcomm. on Tech. and Law of the Senate Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm.*, *available at* 1994 WL 223962 [hereinafter Freeh's Testimony]; *see also EDWIS#1*, 412 F. Supp. 2d at 954; *SDTX#1*, 396 F. Supp. 2d at 763-64 (same).

135 *See supra* notes 85-101 and accompanying text (discussing the minority position).

properly be called 'tracking' information."[136] Second, Mr. Freeh carefully explained that CALEA was in no way intended to enable the government to acquire "information relating to the general location of a cellular telephone . . . ."[137] Third, Mr. Freeh made clear that the purpose of CALEA was to "maintain[ ] . . . the status quo" and that "all telecommunications 'transactional' information" was protected "*exclusively*" by the SCA.[138] Finally, Mr. Freeh noted that CALEA was

---

[136] Freeh's Testimony, *supra* note 134, at *23. Mr. Freeh stated:

> The term "call setup information" is essentially the dialing information associated with any communication which identifies the origin and destination of a wire or electronic communication obtained through the use of a pen register or trap and trace device pursuant to court order. It does not include any information which might disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent whatsoever, with reference to this term, to acquire anything that could properly be called "tracking" information.

Id.

[137] *Id*. at *29. Directly addressing the question of the Pen/Trap Statute, Mr. Freeh stated:

> Some cellular carriers do acquire information relating to the general location of a cellular telephone for call distribution analysis purposes. However, this information is not the specific type of information obtained from "true" tracking devices, which can require a warrant or court order when used to track within a private location not open to public view. Even when such generalized location information, or any other type of "transactional" information, is obtained from communications service providers, court orders or subpoenas are required and are obtained. In order to make clear that the acquisition of such information is not being sought through the use of pen register or trap and trace device, and is not included within the term "call setup information," we are prepared to add a concluding phrase to this definition to explicitly clarify the point: except that such information (call setup information) shall not include any information that may disclose the physical location of a mobile facility or service beyond that associated with the number's area code or exchange.

Id. (citations omitted).

The Eastern District of Wisconsin decision pointed out that the language of Mr. Freeh's proposed change was not the actual language incorporated in the CALEA. *EDWIS#1*, 412 F. Supp. 2d at 956. However, the court noted that "the language which found its way into the law was predicated on the Director's assertion to Congress that, in the government's view, pen register and trap and trace devices were not to be, and would not be, used to secure location information for the cellular phone user." *Id*.

[138] Freeh's Testimony, *supra* note 134, at **28-29 (emphasis added). As noted *supra* notes 55-57, the SCA concerns only stored information. Thus, taking Mr. Freeh's comments as true, a logical inference would be that real time information could never be gained under the SCA's specific and articulable facts standard, as real time information has not been stored. This imposes a significant burden on the government's ability to obtain information absent a search warrant based on probable cause and serves as another reason for the government's stringent utilization of the hybrid theory. As Magistrate Judge Smith stated:

meant "to advance technology, not legal authority . . . ."[139] Any notion that Mr. Freeh's testimony had no effect on the congressional decision to enact CALEA is dispelled by the Act's House Committee Report, paying particular attention to the fact that "[t]he FBI Director testified that the legislation was intended to preserve the status quo, that it was intended to provide law enforcement no more and no less access to information than it had in the past."[140]

The hybrid theory fails on two other grounds: (1) the absence of cross-references and (2) the timing of the respective acts.[141] As Magistrate Judge Smith noted:

> The most glaring difficulty in meshing these disparate statutory provisions is that with a single exception they do not cross-reference one another. The Pen/Trap Statute does not mention the SCA or CALEA; SCA § 2703 does not mention CALEA or the Pen/Trap Statute; and the CALEA proviso does not mention the SCA. CALEA does refer to the Pen/Trap Statute, but only in the negative sense of disclaiming its applicability.[142]

Coupled with the fact that the Acts fail to mention one another in any positive sense, is the equally compelling detail that Congress passed them at various times over a span of fifteen years.[143] Thus, the notion that the CALEA limitation (that the Pen/Trap Statute may not be the exclusive means by which information tending to reveal a user's location can be obtained—effective 1998) was intended by Congress to be circumvented by the SCA (effective 1986) is impossible, as the Pen/Trap

---

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

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

139 Freeh's Testimony, *supra* note 134, at *28.

140 H.R. REP. NO. 103-827(I), at 22 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3509. The report also noted that a goal of the CALEA was to "protect[ ] the privacy of communications." *Id.* at 9. Again, Congress referred to electronic surveillance orders and not a lower standard. *Id.*

141 *See SDTX#1*, 396 F. Supp. 2d at 764.

142 *Id.*

143 *See supra* note 42 (SCA enacted in 1986); *see also supra* note 58 (CALEA enacted in 1994, effective 1998); *supra* note 64 (USA PATRIOT Act enacted in 2001).

Statute was not expanded to include routing information from electronic communications until 2001 by way of the USA PATRIOT Act.[144]

The hybrid theory represents a dramatically flawed governmental attempt to piece together history at the expense of individual privacy, because (1) neither the SCA, CALEA, nor the Pen/Trap Statute were individually intended to grant government access to prospective cell site information; (2) legislative history illustrates that Congress never intended for the government to obtain prospective cell site information absent a showing of probable cause; and (3) the Acts necessary for the hybrid theory fail to mention each other, even when they had fifteen years to do so.

B. Probable Cause Showing

As applied to prospective cell site information, the probable cause standard springs from the definition of a "tracking device," which allows a court, empowered with the ability to issue a warrant for a tracking device, to do so upon a showing of probable cause.[145] In December, 2006, federal magistrate judges received such power by way of the newly revised Federal Rule of Criminal Procedure 41.[146] Like the tracking device definition, Rule 41 requires a probable cause showing before the

---

[144] Magistrate Judge Smith noted the irony:

> If as the government contends all three statutes were necessary for conception, then the statutory authority for this surveillance technique was obviously born *after* the PATRIOT Act amendments of 2001. But this timing undercuts any inference that the CALEA proviso (passed 1994, effective 1998) authorized disclosure of location information under the SCA "specific and articulable facts" standard. What need of subsequent legislation if CALEA already did the trick? On the other hand, if CALEA itself marked the true birth date, then the expanded pen/trap definitions in the subsequent PATRIOT Act are rendered immaterial to the analysis. But without the expanded pen/trap definitions, there is no basis to argue that the Pen/Trap Statute covered cell site data; the old definitions only covered numbers dialed. And without the Pen/Trap Statute's prospective features, so clearly lacking in the SCA scheme, the statutory underpinnings for monitoring of cell phone location simply collapse.

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

[145] 18 U.S.C. § 3117(d) states: "If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction."

[146] FED. R. CRIM. P. 41. The revised rules states that "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." FED. R. CRIM. P. 41(b)(4).

government can receive authorization for the use of a tracking device.[147] Contrary to a showing of specific and articulable facts, a probable cause showing requires the government to "identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used."[148]

Thus, the question becomes whether prospective cell site information is information the government must obtain from a tracking device.[149] Obviously, cellular phones are more closely tied to the individual user's person than a landline telephone.[150] In fact, as early as 1999 Congress indicated that cellular phones presented a threat to individual privacy because they "are normally directly associated with the physical presence of the individual user, and are carried by those users into places where there is a reasonable expectation of privacy."[151] Further, as discussed above, GPS technology and government-mandated 911 capabilities have sparked an increase in the specificity with which a cellular service provider can identify a particular user's location.[152]

---

[147] FED. R. CRIM. P. 41 ("After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant *if there is probable cause* to search for and seize a person or property or to install and use a tracking device.") (emphasis added).

[148] *Id*. BLACK'S LAW DICTIONARY 1239 (8th ed. 2004), defines "probable cause" as

> a reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime. Under the Fourth Amendment, probable cause–which amounts to more than a bare suspicion but less than evidence that would justify conviction—must be shown before an arrest warrant or search warrant may be issued.

[149] A tracking device is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117.

[150] *See For Many People, their cell phone has become their only phone*, USA Today (2003), *available at* http://www.usatoday.com/tech/news/2003-03-24-cell-phones_x.htm (discussing that as of 2003, over 7 million people use only cellular phones with no land line, citing mobility and cost as reasons for the shift).

[151] 145 Cong. Rec. S4033-01, S4048 (daily ed. Apr. 21, 1999), *available at* 1999 WL 230074. The statement came during discussion of the "Electronic Rights (E-RIGHTS) for the 21st Century Act," in which the discussion continued:

> Tracking of cellular telephones, even more-so than automobiles, implicates the movements of a person going about his or her business and personal life. Should the government seek to track a person by surreptitiously placing a mobile tracking device on that person's automobile, a court order would be required based upon a finding of probable cause. No less should be required for use by the government of a wireless telephone as a tracking device.

Id. (citations omitted).

[152] *See* Treglia, *Challenge of Tracking*, *supra* note 2 (discussing the increasing specificity with witch law enforcement can pinpoint and individuals whereabouts by obtaining cell site information and the confusion that results from enforcing twenty-first century

Finally, the most recent push for user location identification cellular phone technology has been the market.[153] The result of these stimuli is that tracking capabilities based on cellular phone technology are

---

technology with eighteenth century legal analysis); Schumann, *supra* note 114, at 9 (analyzing the use of GPS technology as a tool for criminal investigations); Werdegar, *supra* note 7, at 105 (discussing the FCC 911 Act and the government mandate that cellular phones be geographically traceable). Congress also noted governmental influence on tracking capabilities:

> Civil liberties experts have noted that cellular telephone technology "is proceeding in the direction of providing more precise location information, a trend that has been boosted by the rulings of the Federal Communications Commission (FCC) in its "E911" (Enhanced 911) proceeding, which requires service providers to develop a locator capability for medical emergency and rescue purposes." Specifically, the FCC is requiring wireless service providers to modify their systems to enable them to relay to public safety authorities the cell site location of 911 callers. Carriers must also take steps to deploy the capability to provide latitude and longitude information of wireless telephone callers within 125 meters and, ultimately, to locate a caller within a 40-foot radius for longitude, latitude and altitude, to enable locating a caller within a tall building. In a separate proceeding, the FCC in October 1998 proposed ruling that a location tracking capability for wireless telephones was required under the Communications Assistance for Law Enforcement Act (CALEA). The FCC has tentatively concluded that carriers must have the capability of providing to law enforcement a caller's cell site location at the beginning and termination of a call. Whether this capability is ultimately required by the FCC as part of CALEA, *there is no doubt that real-time location information will be increasingly available to law enforcement agencies*.

145 Cong. Rec. S4033-01, S4048 (daily ed. Apr. 21, 1999), *available at* 1999 WL 230074 (citations omitted) (emphasis added).

[153] *See* Phillips, *supra* note 7, at 11-12 (discussing the rise of location-based services and the market forces driving this phenomenon). Phillips, after discussing the emergency response and law enforcement stimuli for location information states:

> Wireless access providers are preparing to . . . for[m] alliances with portals, applications providers and ad servers. . . . More importantly, they are adding real-time location and mobility patterns to the set of data according to which the user's experience is personalized. Geographically specific data may be served in several ways. The user's ISP can be inferred from the IP address. Therefore, since many ISPs are regional concerns, the user's geographic location can be surmised as well. Or the user may explicitly request information pertaining to a specific region, for example, by entering a ZIP code. Or locationally specific content *may be sent only from a particular wireless cell*, much as in a broadcast model. The marketer's ideal, however, is to serve content personalized for each user based on that user's historical profile and *precise, current location*.

Id. (emphasis added).

expanding rapidly, with no clear incentives to stop.[154] Ever-increasing tracking capabilities built into cellular telephones, devices known by Congress to be kept within individuals' clothing, homes, and other private areas, point heavily towards the conclusion that cellular phones, when used by the government to acquire prospective, real time cell site information, fit firmly within the definition of a tracking device.[155]

Courts agree. The Eastern District of New York identified cellular phones as tracking devices because they "revea[l] [a] person's location at a given time."[156] The Southern District of Texas also concluded that "prospective cell site data is properly categorized as tracking device information."[157] The District of Columbia,[158] Maryland,[159] Northern Indiana,[160] and Southern New York[161] districts each agreed that

---

154 *See id*. at 16 ("To summarize, in three different arenas and for three different purposes, the locational surveillance capacity of the wireless telecommunication network is expanding. In each of these arenas, different social values, legal theories and economic structures are called upon.").

155 *See* Farley, *supra* note 23 (concluding that the purpose of the registration is for the cell phone service provider to know the whereabouts of the phone, whether it is roaming or within the home area, and the applicable billing rate according to geographic location of the phone). Whether during the registration process or while receiving information from an active call, what is clear is that cellular phones obviously may be used by the government to "trac[k] the movement of a person . . . ." 18 U.S.C. § 3117.

156 EDNY#1, 384 F. Supp. 2d 562, 564 (E.D.N.Y. 2005).

157 SDTX#1, 396 F. Supp. 2d 747 (S.D. Tex. 2005). The court felt that the mere possibility that Fourth Amendment Privacy rights could be implicated required the data to be so classified, stating: "Because the government cannot demonstrate that cell site tracking could never under any circumstance implicate Fourth Amendment privacy rights, there is no reason to treat cell phone tracking differently from other forms of tracking under 18 U.S.C. § 3117, which routinely require probable cause." *Id*.

158 DDC#3, 407 F. Supp. 2d 134, 140 (D.D.C. 2006) (concluding that in 1994, the government had no knowledge of the high capability cellular phones now have to locate individuals' whereabouts); DDC#1, Nos. 05-403, 05-404, 05-407, 05-408, 05-409, 05-410, 05-411, 2005 WL 3658531, at *1 (D.D.C. Oct. 26, 2005) (adopting the reasoning of the Eastern District of New York and Southern District of Texas decisions).

159 DMD#2, 416 F. Supp. 2d 390, 396 n.9 (D. Md. 2006) ("I am not convinced by the government's argument that the information requested here does not convert a cell phone into a tracking device. The definition of 'tracking device' is broad and contains no articulation of how precise a device must be."); DMD#1, 402 F. Supp. 2d 597, 602 (D. Md. 2005) ("the acquisition of real time cell site information converts a cell phone into a tracking device under 18 U.S.C. § 3117").

160 NDIND, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847, at *4 (N.D. Ind. July 5, 2006) ("converging the Pen Register Statute with the SCA in an attempt to circumvent the exception in the CALEA is contrary to Congress' intent to protect cell site location information from utilization as a tracking tool absent probable cause under the Fourth Amendment").

161 SDNY#2, No. 06 CRIM. MISC. 01, 2006 WL 468300, at *1 (S.D.N.Y. Feb. 28, 2006) (stating that "statutory authority for prospective cell site location information is lacking" and adopting the reasoning of the prior decisions.).

prospective cell site data most closely fits within the tracking device definition, requiring a showing of probable cause. Further, the minority position decisions note the capability of cellular phone tracking, but allow the specific and articulable facts standard for only imprecise general location requests.[162]

Consequently, although there is agreement that cellular telephones can be used as tracking devices, the statutory language as it currently stands opens the door to governmental abuse.[163] Prosecutors are able to piece together statutory language originating over a fifteen-year span, in direct contravention to congressional intent.[164] Because the plain language of the SCA, CALEA, and the Pen/Trap Statute all combine to form a framework that, by its very terms, *could* give government agents authority to gain access to prospective cell site information, some Courts feel obligated to honor the hybrid theory over legislative history clearly to the contrary.[165]

Thus, Congress must clarify the statutory language surrounding the ability of government officials to obtain prospective cell site information.[166] In order to protect individual privacy interests, the most appropriate option is for Congress to mandate a governmental showing of probable cause.

---

[162] *See e.g.*, WDLA, 411 F. Supp. 2d 678, 681 (W.D. La. 2006) ("The Government does not seek (and the court does not authorize the release of) GPS information. The Government also does not seek (and the court does not authorize the release of) cell site information that might be available when the cell phone is off or when no call is made or received. Thus, even if one accepts the argument that a cell phone could be considered a 'tracking device,' the Government's application does not seek tracking information from it."); SDNY#3, No. 06 CRIM. MISC. 01, 2006 WL 3016316, at *9 (S.D.N.Y. Oct. 23, 2006) (accepting the hybrid theory "at least where . . . the government does not seek triangulation information or location information other than that transmitted at the beginning and end of particular calls."); SDNY#1, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005) (allowing prospective, real time cell site information based only on calls made or received by the mobile phone user, from a single tower, and supplied indirectly to the government); *id.* at 445 (noting the tension between the obvious tracking capabilities of cell phones and the electronic communication transmitted by the phone service, noting that the former would require a showing of probable cause and the latter is covered under the SCA).

[163] *See infra* Part IV (suggesting amendments to the current surveillance statutory scheme).

[164] *See supra* notes 125-45 and accompanying text (analyzing the hybrid theory and its flaws).

[165] *See supra* Part II.B.2 (discussing the decisions adhering to the minority position).

[166] *See infra* Part IV (suggesting amendments to the current surveillance statutory scheme).

IV. PROPOSED LEGISLATION

"The proles, normally apathetic about the war, were being lashed into one of their periodical frenzies of patriotism."[167]

Fortunately, this tricky problem is easily fixed. Congress has consistently understood the danger that government acquisition of cellular telephone information presents to individual privacy rights.[168] Where recognition has excelled, however, execution has fallen short.[169] Congress has left judges with a difficult choice: obey a plausible statutory reading of various acts in contravention to congressional intent and privacy rights, or adhere to congressional intent and dispel plain language that possibly grants authority to gain valuable investigatory information.[170] Faced with this decision, judges have split, choosing to adhere to intent when there exists a likelihood of substantial harm to privacy rights and plain language when privacy right infringement seems less severe.[171] Thus, this Note proposes several amendments to the electronic surveillance statutory framework. First, 18 U.S.C. § 2703(d) of the SCA must be amended to clearly exclude any prospective, real time cell site information from the specific and articulable facts standard.[172] Second, 18 U.S.C. § 3117(a) must be clarified to illustrate that Federal Rule of Criminal Procedure 41 is the exclusive means by which a tracking device may be installed in a federal jurisdiction.[173] Finally, 18 U.S.C. § 3117(b) must be amended to reflect that prospective, real time cell site information fits within the definition of a tracking device.[174]

A. Congress Should Amend 18 U.S.C. § 2703(d) as Follows:

> (d) Requirements for court order.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing

---

167 *See* Orwell, *supra* note 1, at 150.

168 *See supra* Part III.B (discussing congressional intent behind the SCA, CALEA, and Pen/Trap Statute).

169 *See supra* Part III.A (discussing the possibility of the hybrid theory due to ambiguous statutory language).

170 *See supra* Parts III.A-III.B (analyzing the hybrid theory and the probable cause approach to government requests for real time cell site information).

171 *See supra* Part III (analyzing the various factors considered when allowing the dual authority position).

172 *See infra* Part IV.A.

173 *See infra* Part IV.B.

174 *See infra* Part IV.B.

> that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. *However, a court may not order disclosure to the government of any prospective, or real time cell site information from any third-party service provider regarding a specific cellular telephone, or any electronic or mechanical device which permits the tracking of the movement of a person or object, absent a showing of probable cause pursuant to Federal Rule of Criminal Procedure 41(d)(1) or a showing of consent from the customer or subscriber.* In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.[175]

Commentary

This addition serves the necessary purpose of ending the dual authority position. A central premise of the hybrid theory was to circumvent the CALEA requirement of an additional authority in order to gain access to electronic communications.[176] However, the addition of the proposed limiting language disallows the chosen method of circumvention, a § 2703(d) order, and forces a governmental showing of probable cause pursuant to Rule 41 in order to obtain prospective, real time cell site information from third party providers.

Also, although the section is non-applicable to state requests, the change will serve as an example to state legislatures, encouraging them to address the problems presented in the federal forum and take a proactive approach to surveillance challenges. Further, the added language leaves open the possibility of subscriber or customer consent absent a showing of probable cause, a central concern to the Southern District of West Virginia, in the situation of a fugitive carrying another user's cellular telephone.[177] The consent exception will balance the privacy rights of cellular telephone subscribers, a chief congressional

---

175 18 U.S.C. § 2703(d). The normal font represents the language of the original statute. The text that appears in italics is the proposed language from the author.

176 *See supra* notes 125-45 and accompanying text (discussing the hybrid theory).

177 *See supra* notes 93-94 and accompanying text (analyzing the Southern District of West Virginia decision and focusing on the lack of a subscriber).

goal of CALEA,[178] with the need of police officers to obtain wholly unknown non-subscriber fugitives by way of cellular technology.[179]

B. Congress Should Amend 18 U.S.C. § 3117(a) as Follows:

> (a) In general.—If a court is empowered to issue a warrant ~~or other order~~ for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside the jurisdiction if the device is installed in that jurisdiction~~.~~ *upon a showing of probable cause pursuant to Federal Rule of Criminal Procedure 41(d)(1).*[180]

Commentary

Already present in the language of § 3117(a) is a demand for authorization of power to install tracking devices within a court's jurisdiction.[181] In December of 2006, federal magistrate judges received such power by way of Rule 41.[182] The proposed language updates the tracking device provision and creates synergy between the two provisions, making it absolutely clear that tracking devices may only be installed pursuant to a showing of probable cause. Further, the subtraction of the phrase "or other order" from the language of the tracking device statute serves to eliminate future attempts by the government to circumvent the requirements of a probable cause showing.

C. Congress Should Amend 18 U.S.C. § 3117(b) and Create 18 U.S.C. § 3117(c) as Follows:

> (b) Definition.—As used in this section, the term "tracking device" means *any device utilized by the government to obtain prospective information or real time information tending to reveal a mobile subscriber's location, or any* electronic or mechanical device

---

178 *See supra* notes 135-40 (discussing former FBI Director Freeh's numerous assertions that CALEA was intended merely to advance technology law, not government interference with privacy).

179 *See supra* note 83 and accompanying text (discussing the applicability of CALEA's exception to only "subscriber[s]").

180 18 U.S.C. § 3117(a). The normal font represents the language of the original statute. The text that appears in italics is the proposed language from the author. The text that is struck through represents the text the author wishes to delete from the statute.

181 *See* FED. R. CRIM. P. 41(a).

182 FED. R. CRIM. P. 41(b)(4) (stating, "a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device").

> which permits the tracking of the movement of a person or object.[183]
>
> *(c) Definition.—As used in this section, the terms "prospective information" and "real time information" mean information acquired by the government after a court order, granted upon a showing of probable cause, authorizing the government to obtain information from a third party service provider, has been signed by a Federal Judge pursuant to Federal Rule of Criminal Procedure 41(d)(1). However, records stored by a third party service provider detailing the past location of a tracking device are deemed "historical information," covered by 18 U.S.C. §§ 2703-2712.*[184]

Commentary

The final change to the tracking device statute leaves no room for prosecutorial disobedience of clear congressional intent. By properly classifying cellular phones used by the government to gain prospective, real time information as tracking devices, the current difficult judicial decision is replaced with clear understanding: If the government seeks real time information tending to reveal a mobile subscriber's location, probable cause must be shown before the court shall grant authorization. The tracking device definition also leaves room for technology growth, as cellular phones will presumably be replaced in the future by new technology. The proposed "tracking device" definition, coupled with the proposed "prospective information" and "real time information" definitions, would apply to all current and future devices maintained by third party service providers with the capability of transmitting location information about a user's whereabouts.

The proposed definitions for "prospective information," "real time information," and "historical information" distinguish information covered under the tracking device statute from that covered under the SCA.[185] Whereas the tracking device statute covers all prospective or real time information (that obtained after a court order pursuant to Rule 41), the SCA is preserved as the correct governing act for all stored or "historical" information.

---

[183] 18 U.S.C. § 3117(b). The normal font represents the language of the original statute. The text that appears in italics is the proposed language from the author.

[184] The text that appears in italics is the proposed language from the author.

[185] *See supra* Part II.A.2 (discussing the SCA, applicable to all stored communications or historical information as opposed to prospective or real time information).

The proposed changes work together to bring the current outdated statutory framework into line with present and future technological advancements. Further, prosecutors may continue to reap the benefits cellular technology provides to law enforcement, while judges have the clear authority to demand that personal privacy rights be upheld. Finally, the highly intrusive nature of cellular telephone information, possibly obtained unbeknownst to the cellular subscriber, is properly categorized as a tracking device requiring a governmental showing of probable cause before being obtained.

V. CONCLUSION

"But it was all right, everything was all right, the struggle was finished."[186]

The proposed changes discussed in Part IV would save Cameron, our unfortunate character in Part I of this Note, from a world of embarrassment, fear, and privacy invasion.[187] Instead of succumbing to the pressure of government agents rushing for the apprehension of a loose criminal, the magistrate judge would require Detective Doe to present probable cause for a warrant search of Cameron's phone. In fact, knowing that such a showing was not feasible based on the current facts, the added protection of a probable cause requirement would force Detective Doe to conduct a thorough investigation, sparing the privacy invasion to nine innocent persons. Cameron would continue on to Chicago and possibly land his dream job, instead of being forced to explain that he was late due to an arrest for murder. Although such slipshod investigations may lead to intermittent lucky finds, Congress has been clear that privacy interests must prevail in this time when technological gains tempt the government to fulfill many of Orwell's darkest visions. With the suggested changes presented above, Congress can present a clear standard of probable cause in conformity with its previous intentions.

Rickey G. Glover[*]

---

186 *See* Orwell, *supra* note 1, at 300.

187 *See supra* Part I (presenting a fictional hypothetical situation).

* J.D. Candidate 2008, Valparaiso University School of Law; B.A., English & General Theater, Appalachian State University, 2005. Special thanks to my mother, my father, Alissa, Chris, and Elisabeth. Also, thanks to David Larry, my first true mentor.