Brooklyn Law Review

Volume 73 | Issue 1 Article 13

2007

The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More Than the Sum of Its Parts?

Timothy Stapleton

The Electronic Communications Privacy Act and Cell Location Data

IS THE WHOLE MORE THAN THE SUM OF ITS PARTS?

I. INTRODUCTION

Cellular phones permit law enforcement to identify their users' locations and track their movements.[1] This is an enormously powerful tool in the hands of police and prosecutors, who have recently used the technology to solve and prosecute high profile crimes.[2] In New York City, the police arrested a night club bouncer after calls from his cell phone placed him near where the body of a murder victim was dumped.[3] In California, the evidence used to convict Scott Peterson of murdering his wife included location data gleaned from his cell phone that undermined his alibi.[4] Perhaps more importantly, other crimes have been prevented from happening.[5] In one case, a thief stole a woman's car with her child and her cell phone inside.[6] The police were able to stop

---

[1] *See* James X. Dempsey, *Digital Search and Seizure: Updating Privacy Protections to Keep Pace With Technology*, *in* SEVENTH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY-DRIVEN WORLD 505 (PLI Pat., Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 8966, 2006). This data is collectively referred to as "cell site data" or "cell site information" by various cases and commentators. This Note will refer to data taken from the transmissions of a cell phone that reveal the phone's physical location as "cell location data." There are different types of this data, each of which has different features and may require its own legal analysis. When referring to these specific types of cell location data, this Note will use a term that indicates what type is being discussed. *See infra* Part II.

[2] Stephen V. Treglia, *Trailing Cell Phones*, N.Y. L.J., July 18, 2006, at 5.

[3] Nancie L. Katz, *Bouncer Pleads Not Guilty in Death of Graduate Student*, N.Y. DAILY NEWS, Mar. 23, 2006.

[4] Diana Walsh & Stacy Finz, *The Peterson Trial: Defendant Lied Often, Recorded Calls Show Supporters Misled About Whereabouts*, S.F. CHRON., Aug. 26, 2004, at B1.

[5] Treglia, *supra* note 2.

[6] *Girl, 5, Found Safe as Man Steals Car*, ROCKY MOUNTAIN NEWS, Apr. 22, 2004, at A18 [hereinafter *Girl, 5*]; *see also* Treglia, *supra* note 2 (citing this incident as an example of how "cell phone mapping" has prevented crimes in progress).

the car and rescue the child within thirty minutes by tracking the woman's cell phone.[7] Yet with each increase in law enforcement's power to conduct surveillance comes an increased concern for individual privacy. Numerous commentators have expressed concern over the ease with which the government has accessed data from individuals' cell phones that reveals their whereabouts and permits real-time tracking.[8]

There is currently no federal statute that explicitly strikes the balance between privacy and the needs of law enforcement in the context of cell phone tracking.[9] Moreover, unless police surveillance discloses that the target was at home when his or her cell phone transmissions were monitored, the Fourth Amendment appears to provide no protection.[10] It seems that prior to August of 2005 law enforcement agencies requested, and were routinely granted, the authority to access cell location data with minimal judicial oversight.[11] In that month, a federal district court in New York, after soliciting an amicus brief from privacy advocates, issued an opinion denying the government's application for access to an individual's cell location data and stated that it would not grant any such application without a showing of probable cause.[12] Since then, a slew of district courts have considered whether the Electronic

---

[7] *Girl, 5*, *supra* note 6.

[8] *See* Dempsey, *supra* note 1, at 529, 537 (noting that until recently the government routinely received cell site information on a less than probable cause basis); JAY STANLEY, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESS AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY 14 (2004), *available at* http://www.aclu.org/FilesPDFs/surveillance_report.pdf; Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 RICHMOND J.L. & TECH. 16, 16 (2007); *see also* M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2006) (noting the advantages of cell phone tracking for law enforcement); Stephanie Lockwood, Recent Development, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 311 (2004).

[9] *See* Dempsey, *supra* note 1, at 533.

[10] *See infra* notes 44-47 and accompanying text.

[11] Dempsey, *supra* note 1, at 537.

[12] *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information (*E.D.N.Y. I*), 384 F. Supp. 2d 562, 563-64 (E.D.N.Y. 2005). At the very least, prior to *E.D.N.Y. I*, there were no published opinions denying such applications. Because the names of the published cases are extremely unwieldy, this Note will refer to the cases by the jurisdiction in which they were decided. Where a single jurisdiction has produced more than one published opinion, a Roman numeral will indicate the opinion's chronological position within that jurisdiction's published opinions.

Communications Privacy Act of 1986 ("ECPA"), taken together with the Communications Assistance for Law Enforcement Act of 1994 ("CALEA") and the Stored Communications Act ("SCA"), permits the government to compel a phone company to disclose such information on a lesser showing than probable cause, or whether the government must obtain a warrant to access cell location data.[13] A majority of the cases have held that a warrant is required for the contested types of data, although they have produced varying analyses of the issue.[14]

This Note argues that a warrant issued upon probable cause is the appropriate form of authorization for law enforcement to conduct certain types of surveillance made possible by cell location data.[15] To reach that conclusion, this Note analyzes the leading opinions to date and concludes that the government's argument is irredeemably flawed. Part II of this Note discusses the technology of cellular telephony, with a special emphasis on the features of cellular phones that reveal their users' locations. Particular emphasis is placed on identifying the different kinds of data that can be gleaned from cell phone transmissions. Part III explains the statutory and

---

[13] *See, e.g.*, *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (*Texas I*), 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) (denying government request); *In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information (*E.D.N.Y. II*), 396 F. Supp. 2d 294, 295 (E.D.N.Y. 2005) (denying government request); *In re* Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information (*Texas II*), 433 F. Supp. 2d 804 (S.D. Tex. 2006) (granting government's request); *In re* Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking (*Texas III*), 441 F. Supp. 2d 816, 837 (S.D. Tex. 2006) (denying government request); *In re* Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace (*S.D.N.Y. I*), 405 F. Supp. 2d 435, 436 (S.D.N.Y 2005) (approving government request). For a discussion of probable cause and the warrant requirement, see *infra* note 51.

[14] This Note will confine its discussion, to the extent possible, to the opinions of Magistrate Judge Smith in the Southern District of Texas (*Texas I* and *Texas III*), and the single opinion of Magistrate Judge Gorenstein (*S.D.N.Y. I*). These opinions offer the most cogent analyses of the competing theories. For a discussion of these cases, see *infra* Part IV. As of this writing, the other cases that have rejected law enforcement's arguments include: *In re* Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information (*E.D. Wis.*), No. 06-Misc-004, 2006 WL 2871743, at *5 (E.D. Wis. Oct. 6, 2006); *In re* Application for an Order Authorizing the Installation and use of a Pen Register and Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the Number [Sealed] (*Maryland III*), 439 F. Supp. 2d 456, 456-57 (D. Md. 2006).

[15] For a discussion of tracking devices and the probable cause requirement, see *infra* note 51 and accompanying text.

constitutional context of the "cell site cases." This discussion highlights the features of federal legislation that law enforcement and privacy advocates have used in making their respective arguments. Part IV analyzes the cases that have considered law enforcement applications to obtain cell location data and offers a critique of the analyses the cases have produced. Part V concludes the Note by suggesting statutory amendments that would remediate the ambiguities in the statutes and address the policy concerns raised by warrantless cell phone monitoring.

II. TECHNOLOGICAL BACKGROUND

Wireless telephony operates through a network of cell towers that emit radio frequencies capable of carrying the human voice and other data.[16] Cell towers operate much like a conventional radio tower, but emit radio frequencies at a comparatively low power.[17] The same frequencies, therefore, can be used by a nearby tower without having the signals from one tower interfere with those of another.[18] This innovation is at the core of cellular technology, permitting many people in a relatively small area to communicate using the same radio frequencies.[19] Because there will be a greater number of users in densely packed urban areas than in rural and suburban areas, cell towers are much closer together in big cities.[20] The cells themselves are thought of as hexagonal zones, with a cell tower sitting wherever three hexagons meet.[21] The spot at which the cell tower sits is referred to as the "cell site."[22] Each cell might therefore be serviced by six different towers, any one or all of which could pick up the signal of a phone located

---

[16] *See* Marshall Brain & Jeff Tyson, How Cell Phones Work, *available at* http://www22.verizon.com/about/community/learningcenter/articles/displayarticle1/0,,1008z1,00.html (last visited Sept. 8, 2007). The present controversy deals with police surveillance via conventional wireless telephony and does not involve Global Positioning Systems ("GPS") technology. Although related, the legal questions those technologies pose are distinct from the ones present in the cell location cases.

[17] *Id.*

[18] *Id.*

[19] *Id.* Radio frequencies are a naturally limited resource. *Id.*

[20] *See* Tom Farley & Mark van der Hoek, *Cellular Telephone Basics*, Jan. 1, 2006, http://www.privateline.com/mt_cellbasics/index.html.

[21] *Id.*

[22] *Id.*

within the cell.[23] The area within a cell that is serviced by a particular tower is a "cell sector."[24]

Cell phones are in near-constant communication with surrounding cell towers.[25] When turned "on" a cell phone automatically searches for the strongest signal available.[26] Once the phone selects the best signal, it transmits the user's identifying data (the subscriber's ten-digit phone number and a thirty-two-digit number unique to the phone itself), so that the subscriber's network knows how to route incoming calls, and so that the cell tower can "hand off" the user's phone to another tower if that tower can provide better reception.[27] This process is called "registration" and takes place every seven seconds.[28] Data generated during registration ("registration data") is one of several kinds of cell location data that law enforcement might use to locate an individual without listening in on any of her communications.[29] Cell site data, because it only identifies the individual cell tower with which the phone is communicating, can reveal only the general location of the user.[30] Other features of wireless telephony, however, permit law enforcement to pinpoint the user with much greater accuracy.

One of these features is the "facing." The typical cell tower has three sets of panels, each of which sends and receives signals in a 120-degree arc.[31] It is possible to determine which set of panels, or "face" is communicating with a subscriber's cell phone, thereby indicating which third of the tower's circumference contains the target phone ("facing data").[32] Law enforcement can also ascertain the strength of a cell phone signal ("signal strength data"), which increases as the phone

---

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.* Registration establishes the "control channel," the two frequencies the phone and tower use to guide incoming and outgoing calls through the network. It is important to note that the control channel does not carry any content of the communications sent by the cell user. Even once the phone is registered, the phone continues to send its identifying information every seven seconds, in part to make sure that the hand off to another cell tower is seamless. *See Texas I*, 396 F. Supp. 2d at 750-51.

[29] *See Texas I*, 396 F. Supp. 2d at 751.

[30] *S.D.N.Y. I*, 405 F. Supp. 2d at 449; *see also* Farley & van der Hoek, *supra* note 20.

[31] Farley & van der Hoek, *supra* note 20.

[32] *Id.*

gets nearer to the tower and decreases as it goes farther away.[33] A cell phone's location can be determined still more precisely by a process called "triangulation."[34] Triangulation compares information from multiple towers, measuring either the angle at which the phone's signal strikes the towers' faces or the difference in time it takes the signal to reach the different towers.[35] All of this data is produced as the phone registers and reregisters, as well as at the beginning and end of each call made and received ("initiation/termination data").[36]

There is one final aspect of the technology that is crucially important: cell phone companies store all this data.[37] Law enforcement may request that a service provider turn over the cell location data it has stored among its subscriber records ("historical data") or that the service provider turn over records on an ongoing basis ("prospective data").[38] It is this latter type of data that permits real-time tracking of individuals.[39]

In sum, cell location data can reveal a user's position with varying degrees of precision depending on the concentration of cell towers in a given area and the type of information that law enforcement is able to access.[40] Law enforcement can request data sets defined by the precision with which they can locate the subject phone (cell site, facing, signal strength, and triangulation data) or based on the process that generated the signals (initiation/termination data and

---

[33] *See* Brain & Tyson, *supra* note 16.

[34] Lockwood, *supra* note 8, at 308 (cited in *Texas I*, 396 F. Supp. 2d at 751 n.5).

[35] *Id.* at 308-09. It is important to note the differences in precision with which each data set is capable of locating a phone. The government has argued, and some courts have accepted, that a warrant is not required to locate and/or track suspects if the monitoring is done with less precision. *See S.D.N.Y. I*, 405 F. Supp. 2d at 449; *see also* Dempsey, *supra* note 1, at 537. (Data taken from triangulation techniques will be referred to as "triangulation data.")

[36] Farley & van der Hoek, *supra* note 20. As with data produced during registration, the signals at the beginning and end of the call do not carry any content of the communications. If law enforcement were to access call initiation/termination data, but not registration data, then it could only spot check a person's whereabouts, rather than monitor his or her movements for an extended period of time.

[37] *See In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [Sealed] and [Sealed] and the Production of Real Time Cell Site Information (*Maryland I*), 402 F. Supp. 2d 597, 599 (D. Md. 2005).

[38] *Id.*

[39] *Id.* (noting that "real-time data" is a subset of prospective data).

[40] Because there are several different types of data sets at issue in this controversy, "cell location data" will be used as a blanket term to refer to any data that permits law enforcement to locate or track an individual using cell phone signals. "Cell site data" will refer to cell location data from a single cell tower.

automatic registration data.)[41] A data set that includes triangulation and signal strength data permits the tracking of an individual with the greatest possible degree of precision, while cell site data can indicate only generally where a target is or was located. Initiation/termination data can reveal the phone user's location at the time he or she made or received a call, while registration data can betray the user's location at all times the phone was turned on. Finally, all of the data sets can be made available as historical data (data which exists in phone company records prior to the time a court order compelling its disclosure is issued) or as prospective data (data not in existence when the order is issued, but which is turned over to law enforcement on an ongoing basis throughout the time period set out in the order).[42] The types of data law enforcement sought in the various published decisions have affected the courts' decisions to grant or deny law enforcement access to it, although as this Note argues, the only distinction that matters under the ECPA, properly construed, is the distinction between historical and prospective data.[43]

III. THE LEGAL FRAMEWORK

The Fourth Amendment does not protect information that is voluntarily disclosed to third parties.[44] Because cell phone users disclose their location to the phone company in order for the company to process their calls, there is probably no constitutional protection for most cell location data.[45] The Fourth Amendment only prohibits warrantless surveillance of

---

[41] *See supra* notes 31-36 and accompanying text.

[42] *See Maryland I*, 402 F. Supp. 2d at 599.

[43] *See infra* notes 160-171 and accompanying text.

[44] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (records of phone calls held by phone company); United States v. Miller, 425 U.S. 435, 443 (1976) (financial records held by bank); Couch v. United States, 409 U.S. 322, 335 (1973) (financial and tax records held by accountant); Hoffa v. United States, 385 U.S. 293, 302 (1966) (statements made to confidential informant); *see also* Orin S. Kerr, *A User's Guide To The Stored Communications Act, and a Legislator's Guide To Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004).

[45] One magistrate involved in this controversy adopted a rather narrow view of the voluntarism of cell site transmissions, stating that at least with regard to automatically generated registration data, the phone user cannot be said to have "voluntarily conveyed" cell site data to the phone company. *Texas I*, 396 F. Supp. 2d at 756-57. Another court differed, noting that "the individual has chosen to carry a device and to permit transmission of its information to a third party, the [phone service] carrier." *S.D.N.Y. I*, 405 F. Supp. 2d at 449-50. If the former analysis is correct, there may be a cognizable Fourth Amendment claim to protect registration data.

suspects in their homes.[46] Constraints on government acquisition of cell location data (and many other forms of electronic surveillance) are therefore primarily statutory—a state of affairs that is consistent with the history of electronic surveillance law.[47]

Given the lack of constitutional protection, one might find it surprising that there is currently no statute that explicitly regulates governmental access to cell location data.[48] Grappling with the ambiguities in existing electronic surveillance laws, courts have asked whether prospective cell location data should be treated like the data provided by a tracking device installed by the police, or rather, whether the data should be treated like subscriber records, such as the record of numbers dialed by the target phone.[49] If cell location data is treated like a tracking device, then governmental access to it is governed by 18 U.S.C. § 3117, enacted as part the ECPA.[50] A warrant issued pursuant to probable cause would then be required (in most instances) to locate or track an individual using his or her cell phone.[51] If cell location data is better analyzed as a form of "subscriber record," then law

---

[46] *Compare* United States v. Karo, 468 U.S. 705, 716-17 (1984) (Fourth Amendment requires a warrant to monitor a tracking device that is within the target's home), *with* United States v. Knotts, 460 U.S. 276, 282 (1983) (no warrant required if a tracking device is monitored while the target in on public roads.).

[47] *See* Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 72 (2006) (noting that, although the customary view is to see the judiciary turning the "constitutional ratchet" to provide greater protection for civil liberties than legislatures would require, Congress found itself providing more privacy protection from electronic surveillance than the Fourth Amendment required throughout most of the Twentieth Century.)

[48] *See* Dempsey, *supra* note 1, at 533.

[49] *See, e.g.*, *Texas I*, 396 F. Supp. 2d at 750, 753. What might have been a more straightforward debate over the proper statutory interpretation is complicated by the fact that cell location data provides the same information as tracking devices while taking the form of subscriber records. Cell location data is therefore amenable to both analogies.

[50] Pub. L. No. 99-508, 100 Stat. 1848 (1986).

[51] The law governing tracking devices is not entirely settled. Although a warrant is not constitutionally required to install and monitor a tracking device so long as the target remains in the public realm, it is usually impossible for government agents to know in advance whether a tracking device will disclose that the target is in a space, such as the home, where he or she enjoys a reasonable expectation of privacy. The Fourth Amendment requires the government to obtain a warrant issued pursuant to probable cause in order to engage in such surveillance. *Karo*, 468 U.S. at 716-17. Because of the uncertainty over what the tracking device will reveal, the prudent magistrate will insist on a showing of probable cause before authorizing the installation of such a device. *See Texas I*, 396 F. Supp. 2d at 751-52; JAMES G. CARR & PATRICIA L. BELLIA, 1 THE LAW OF ELECTRONIC SURVEILLANCE § 4:83, at 4-207 (West 2007).

enforcement needs only to obtain a court order upon a showing of "specific and articulable facts" demonstrating relevance to an ongoing criminal investigation, per the terms of the SCA.[52] This is a much lighter burden for law enforcement to meet.[53] Law enforcement agencies argue for the lighter burden of proof, advancing a "hybrid theory" that combines two distinct grants of authority found in different statutes to authorize cell location/tracking, which neither statute recognizes on its own.[54]

A final consideration when analyzing the appropriate legal framework is that the provisions of the SCA alone appear to be sufficient to grant law enforcement access to historical cell location data.[55] The present controversy therefore deals with a question that is significantly narrower than whether law enforcement may access cell location data without a warrant. More precisely, the question is whether *prospective* cell location data (from the very general "cell site data" to the very precise "real-time triangulation data") is accessible by law enforcement subject to the same strictures that govern the use of conventional tracking devices.[56] The arguments advanced by law enforcement agencies and by privacy advocates have addressed this precise question.

A. Law Enforcement's "Hybrid Theory"

The government has claimed statutory authority to access cell location data under a theory that combines the authority granted by multiple statutes.[57] The hybrid theory posits that federal district courts have the authority to compel the disclosure of prospective cell location data when they issue an order for a pen register[58] in conjunction with an order for stored subscriber records.[59] Advocates of this theory argue that it fulfills the intent of Congress as expressed in the ECPA and

---

[52] 18 U.S.C. § 2703(d) (2006).

[53] *See infra* notes 64-69 and accompanying text.

[54] *See Texas I*, 396 F. Supp. 2d at 758 n.13; *see also infra* Part IV.A.

[55] *See Maryland I*, 402 F. Supp. 2d at 600.

[56] For a discussion of the law regarding tracking devices, see *supra* note 51 and accompanying text.

[57] The term "hybrid theory" was first used in *Texas I*, *see* 396 F. Supp. 2d 747, 758 n.13.

[58] A pen register is the device that law enforcement agents use to record the "dialing, routing, addressing, or signaling information" transmitted by the target phone. *Texas I*, 396 F. Supp. 2d at 761 n.17 (quoting 18 U.S.C. § 3127(3) (2006)).

[59] *Id.* at 761.

harmonizes the text of the relevant statutes to form a coherent scheme of surveillance regulation.[60]

The first building block of the hybrid theory is the Pen/Trap Statute.[61] The Pen/Trap Statute is part of Title III of the ECPA.[62] It governs the installation and use of pen registers and trap/trace devices.[63] The USA PATRIOT Act added the term "signaling information," expanding the pen register's previous scope to encompass all signaling information transmitted as part of an electronic communication.[64] The Pen/Trap Statute provides that a judge "shall enter an ex parte order" compelling the cooperation of an electronic communications service provider where a government attorney has certified that the information likely to be obtained from the pen/trap device is "relevant to an ongoing criminal investigation."[65] This limited form of review exists "merely to safeguard against purely random use of [pen and trap/trace] device[s],"[66] while ensuring that the devices are promptly available to law enforcement agencies.[67] "Certified relevance" is the lowest evidentiary burden the ECPA imposes upon law enforcement.[68] Orders for pen/trap devices are the only ones that may be issued on such a minimal showing.[69] Pen/trap authority is granted with minimal judicial oversight because

---

[60] *S.D.N.Y. I*, 405 F. Supp. 2d at 448-49.

[61] *See id.* at 438.

[62] *Texas I*, 396 F. Supp. 2d at 752.

[63] *Id.* A pen register records the numbers of all outgoing calls made by the target phone, as well as the time and duration of those phone calls. A trap/trace device records the numbers of all phones that place calls to the target phone. *Id.*; *see also* 18 U.S.C. § 3127(3)-(4) (2006).

[64] USA PATRIOT ACT of 2001, Pub. L. No. 107-56, § 216(c)(2), 115 Stat. 272, 288-90 (codified as amended at 18 U.S.C. § 3127(3) (2001)). ("USA PATRIOT Act" is an acronym for the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.) This amendment is important to hybrid theory advocates, because "signaling information" can potentially cover automatic registration data, whereas dialing, routing and addressing information cannot. Because registration data permits law enforcement to track cell phones even when there is no call in progress, its accessibility greatly increases the government's power to engage in surveillance. *See S.D.N.Y. I*, 405 F. Supp. 2d at 438-39; *see also supra* notes 25-36 and accompanying text.

[65] 18 U.S.C. § 3123(a)(1) (2006).

[66] United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).

[67] CARR & BELLIA, *supra* note 51, § 4:81, at 4-200 to -201; *see also In re* Application of the United States of America for an Order Authorizing Installation and Use of a Pen Register and Trap and Trace Device, 846 F. Supp. 1555, 1559 (M.D. Fla. 1994).

[68] *Texas I*, 396 F. Supp. 2d at 753.

[69] *See id.*

Congress believed that the disclosure of this information is minimally invasive.[70]

Because the target phone transmits cell location data, pen registers, not trap/trace devices identify the phone user's location.[71] If the hybrid theory correctly asserts that cell location data is "dialing, routing, addressing, or signaling information,"[72] then the terms of the Pen/Trap Statute alone permits law enforcement to access cell location data on a showing of certified relevance. There is, however, an exception to the Pen/Trap Statute, codified elsewhere in the United States Code, which regards cell location data.[73] The language of this exception clearly prevents cell location data from being disclosed to law enforcement under the authority of the Pen/Trap Statute and, therefore, on the minimal showing of certified relevance:

> [W]ith regard to information acquired *solely pursuant to* the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) . . . .[74]

The hybrid theory relies on the language "solely pursuant to" for the assertion that Congress intended the Pen/Trap Statute, supplemented by some other, unspecified form of authority, to permit cell phone location and tracking.[75] The semantic implication of the term "solely" becomes the lynchpin in the government's argument; if the word were not there, it would be clear that Congress forbade the use of pen registers to obtain cell location data. Because Congress did include the phrase "solely pursuant to," the government's argument that "signaling information," per the Pen/Trap Statute, is accessible by law enforcement when conjoined with some other statutory grant of authority has a plausible textual

---

[70] *See Texas III*, 441 F. Supp. 2d at 830 ("Legal process [under the ECPA] is calibrated to the degree of intrusion. So 'the greater the privacy interest at stake, the higher the [evidentiary] threshold Congress uses.'" *Id.* at 829 (quoting Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT ACT: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 620-21 (2003)).

[71] *See S.D.N.Y. I*, 405 F. Supp. 2d at 439 n.2.

[72] *See* 18 U.S.C. § 3127(3) (2006).

[73] *Id.* at 440.

[74] 47 U.S.C. § 1002(a)(2)(B) (2006) (enacted as part of CALEA) (emphasis added).

[75] *S.D.N.Y. I*, 405 F. Supp. 2d at 442.

basis.[76] The other grants of authority that the ECPA provides are included in the provisions governing wiretaps,[77] tracking devices[78] and stored communications and subscriber records such as email.[79] Proponents of the hybrid theory argue that the SCA provides the compliment to pen register authority, as required by the "exception clause."[80] From the government's perspective, the SCA is an attractive candidate for this role because, after the Pen/Trap Statute, the SCA places the lowest evidentiary burden on the law enforcement agency seeking such an order.[81] It is also a textual fit; the critical section providing in pertinent part:

> [A governmental entity may require a provider of electronic communication service] to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) . . . if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.[82]

This final step in the hybrid theory fits together with the Pen/Trap Statute because of the breadth of the terms "records or other information." Cell location data could fairly be conceptualized as "other information."[83] Various federal courts have accepted this theory, issuing orders for the release of stored communications (under the SCA) and for the use of a pen register (under the Pen/Trap Statute) to access prospective cell location data.[84]

In summary, the government's hybrid theory seeks the authority to locate and track individuals on a prospective basis (as opposed to simply determining where they have been in the past) by accessing the data gleaned from their cellular phone transmissions. Although it is conceptually coherent to think of this data as analogous to the dialing and addressing records

---

[76] *S.D.N.Y. I*, 405 F. Supp. 2d at 443.

[77] 18 U.S.C. §§ 2510-2522 (2006); *see also* Kerr, *supra* note 69, at 620 (referring to the authority for a wiretap as a "superwarrant").

[78] 18 U.S.C. § 3117; *see also Texas I*, F. Supp. 2d at 752.

[79] 18 U.S.C. § 2703(d) (requiring an intermediate showing of "specific and articulable facts") (enacted as part of the SCA).

[80] *S.D.N.Y. I*, 405 F. Supp. 2d at 448-49.

[81] *Texas I*, 396 F. Supp. 2d at 753

[82] 18 U.S.C. § 2703(c)-(d) (2006).

[83] *See S.D.N.Y. I*, 405 F. Supp. 2d at 444-48.

[84] *See infra* Part IV.

accessible by a pen register, Congress has unambiguously forbidden the Pen/Trap Statute, standing alone, to authorize cell phone tracking. The SCA (the *Stored* Communications Act), clearly authorizes the disclosure of historical cell location data but cannot, by its terms, compel the disclosure of prospective data.[85] Because prospective cell data, especially data obtained in real-time, is much more valuable to law enforcement, the government has sought to combine the forward-looking grant of authority found in the Pen/Trap Statute with the authority to access "subscriber records" granted by the SCA in order to overcome the prohibition against using the Pen/Trap Statute as the sole authority for locating individuals.[86] Accepting the hybrid theory means accepting that the Pen/Trap Statute and the SCA, taken together, grant the government more power to conduct electronic surveillance than either statute grants on its own.

B. Privacy Advocates' Tracking Device Theory

Those who oppose law enforcement access to cell location data on a showing of specific and articulable facts argue very simply that, "[w]hile the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell [location] data."[87] Under this theory, the portion of the ECPA dealing with tracking devices governs access to prospective cell location data.[88] The term "tracking device" is defined in that section as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[89] As noted by one magistrate, the statute regulating the use of tracking devices applies to a device even if it is not designed to be a tracking device and even if it serves some purpose other than the locating or tracking of individuals; the statute applies so long as a device *permits* the tracking of the movement of a person or object.[90] The same judge observed that 18 U.S.C. § 3117 makes no mention of the precision with which law enforcement may

---

[85] *Texas I*, 396 F. Supp. 2d at 759, 759 n.16.

[86] *Id.* at 761.

[87] *Id.* at 754.

[88] 18 U.S.C. § 3117 (2006).

[89] *Id.*

[90] *Texas I*, 396 F. Supp. at 753.

locate the device in question.[91] It is therefore irrelevant, for the purposes of § 3117, whether law enforcement applies for real-time triangulation data or cell site data turned over on an ongoing basis.[92] It might also be noted that the definition of a tracking device covers a device used simply to locate a target, as long as the device *permits* the tracking of the target's movement. Once a court accepts that a cell phone is converted to a tracking device when law enforcement accesses the user's cell location data, § 3117 is triggered and law enforcement should apply for a warrant to obtain the data.[93]

The preceding discussion delineated the relevant contours of federal electronic surveillance law and offered a summary of the two theories competing to govern cell location data. The plain language of the relevant statutes makes cell location data amenable to both the hybrid and the tracking device theories of the ECPA. A decision about which theory produces the rule that strikes the right balance between privacy and the needs of law enforcement requires a closer examination of the opinions that have analyzed the competing theories.

IV. THE CELL LOCATION CASES

The difficulty that courts face in the cell location cases would be understandable if they were confronted only with the vagaries of the ECPA. The cases are more vexing still because law enforcement has sought various different types of cell location data in different cases, and certain courts have found the differences persuasive.[94] Courts on both sides of the controversy have been embroiled in an effort to produce the correct textual analysis of the relevant statutes, combining interpretive virtuosity with a growing record of legislative history. The following is a closer analysis of the two theories, viewed through the opinions adopting and rejecting them.

---

[91] *Texas I*, 396 F. Supp. at 753.

[92] *See supra* notes 40-42 and accompanying text.

[93] *See supra* note 51.

[94] *See* Dempsey, *supra* note 1, at 537; *see also Texas III*, 441 F. Supp. 2d at 827.

A. Cases Accepting the Hybrid Theory

Magistrate Judge Gorenstein in the Southern District of New York decided the primary case accepting the hybrid theory.[95] This is the minority rule, with only four other federal magistrates joining the analysis in published opinions.[96] Cases following this opinion have made little use of the tools of statutory interpretation other than a plain reading of the statutory texts. They do rely to some extent on the legislative history behind the statutes, including the testimony of former FBI Director Louis Freeh, appearing before Congress to support the passage of CALEA.[97] Yet the success of the hybrid theory seems to depend primarily on its textual analysis of the relevant statutes. This textual analysis needs to demonstrate that the transmissions from cellular phones are best thought of as being both "dialing, routing, addressing, or signaling information" in order for the Pen/Trap Statute to apply and as a form of "[subscriber] record or other information" in order for the SCA to apply.[98] Courts in the hybrid camp also need to interpret the "exception clause" as the link that combines the authority granted by the two statutes.[99]

An order for the installation of a pen/trap device permits the capture of all "dialing, routing, addressing, or signaling information" transmitted by the target phone for a period of up

---

[95] *S.D.N.Y. I*, 405 F. Supp. 2d at 439.

[96] *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone (*S.D.N.Y. III*), 2006 WL 3016316, No. 06 Crim. Misc. 01 (S.D.N.Y. Oct. 23, 2006); *Texas II*, 433 F. Supp. 2d 804 (S.D. Tex. 2006); *In re* Application of the United States of America 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 (*W. Va. Opinion*), 415 F. Supp. 2d 663 (S.D. W. Va. 2006); *In re* Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information (*La. Opinion*), 411 F. Supp. 2d 678 (W.D. La. 2006). The *W.Va. Opinion* is exceptional for recognizing that the exception clause in 47 U.S.C. § 1002 does not apply to the tracking of an individual who is carrying a cell phone but is not the subscriber of the phone service. *Id.* at 665-66. In jurisdictions accepting the hybrid theory, law enforcement may therefore track a phone that is not in the possession of the subscriber pursuant to the authority in the Pen/Trap Statute and on the minimal showing of certified relevance required by that statute. For a full discussion of this point, see *infra* notes 153-159 and accompanying text.

[97] *See, e.g.*, *S.D.N.Y. I*, 405 F. Supp. 2d at 443; *La. Opinion*, 411 F. Supp. 2d at 681. For a discussion of Director Freeh's testimony, see *infra* text accompanying notes 177-191.

[98] *See S.D.N.Y. I*, 405 F. Supp. 2d at 438-40; 18 U.S.C. §§ 2703(c), 3127(3) (2006).

[99] *Id.* at 440-43; *see also supra* text accompanying notes 71-76.

to 60 days from the date the order is issued.[100] Courts upholding the hybrid theory must first accept that cell location data qualifies as such information. The support for this first step, as analyzed in *S.D.N.Y. I*, comes from the fact that cell phones transmit a signal to cell towers.[101] The term "signaling information," then, covers "information on the location of cell towers used by a cellular telephone."[102] The court in *S.D.N.Y. I* used the legislative history of the USA PATRIOT Act, which added the term "signaling information" to the definition of a pen register, in order to buttress its conclusion that the term was meant to cover signals transmitted by cell phones.[103] That history reveals an intention that the term would have a broad sweep, stating that "'signaling information' would 'apply across the board to all communications media.'"[104]

The court's other argument for bringing cell location data under the aegis of the Pen/Trap Statute stems from a pre-USA PATRIOT Act case from the Court of Appeals for the District of Columbia, in which the court found that signals from a cell phone "which are necessary to achieve communications between the caller and the party he or she is calling, clearly are 'signaling information.'"[105] The court in *S.D.N.Y. I* presumed that Congress was aware of the interpretation that the *U.S. Telecom* court gave to the term "signaling information" and intended to incorporate that interpretation into the USA PATRIOT Act.[106]

---

[100] 18 U.S.C. §§ 3123(c), 3127(3) (2006); *see also S.D.N.Y. I*, 405 F. Supp. 2d at 438 n.1 (noting that in the past the use of a pen register required the actual installation of a physical device, but that, at least in the Southern District of New York, the same information is conveyed by the telephone service provider in a digital format, and that the same standards govern, regardless of the form the data takes).

[101] *S.D.N.Y. I*, 405 F. Supp. 2d at 438-39.

[102] *Id.* at 439.

[103] *Id.*

[104] *Id.* (citing H.R. Rep. No. 107-236(I), 107th Cong., 1st Sess. (2001.)). This reading of the legislative history is contrary to the analysis performed by the court in *Texas I*, which "note[d] an absence of legislative history indicating that Congress intended cell data to be included in this term when it enacted the USA PATRIOT Act." *Id.* at 439 (citing *Texas I*, 396 F. Supp. 2d at 761).

[105] *S.D.N.Y. I*, 405 F. Supp. 2d at 439 (citing U.S. Telecomm. Ass'n v. FCC, 227 F.3d 450, 464 (D.C. Cir. 2000)). At issue in the *U.S. Telecom* litigation, inter alia, was the FCC's interpretation of this term—in accepting this definition, the D.C. Court upheld the FCC interpretation. *U.S. Telecom Ass'n*, 227 F.3d at 453.

[106] *S.D.N.Y. I*, 405 F. Supp. 2d at 439 (citing and quoting Lorillard v. Pons, 434 U.S. 575, 581 (1978) for the proposition that "[w]here . . . Congress adopts a new law incorporating sections of a prior law, Congress normally can be presumed to have had knowledge of the interpretation given to the incorporated law, at least insofar as it affects the new statute.").

The next step in the hybrid theory analysis is to find the authority needed to supplement the Pen/Trap Statute in § 2703 of the SCA.[107] The broad language contained in that section of the SCA makes this step a fairly easy one, and there is little dispute that historical cell location data could be accessed with this authority alone.[108]

The final step for law enforcement to take in order to gain access to prospective cell data on a showing of "specific and articulable facts" is to interpret the exception clause codified by CALEA.[109] It is critical to the success of the hybrid theory that the language "solely pursuant to the authority for pen registers" be read to mean "pen registers and some other form of authority in the ECPA."[110] This is so because the *S.D.N.Y. I* court, and those that follow it, state not only that the hybrid theory is a plausible interpretation of the electronic surveillance laws, but also the only one possible.[111] It appears that the advocacy group appearing as *amicus* in *S.D.N.Y. I* had argued that the exception clause in § 1002 should be read as "a simple direction that no cell site information may be obtained pursuant to the Pen Register Statute."[112] The structural problem with this argument, according to the court, is that if cell location data is not accessible via a pen register, then it must not be accessible by law enforcement at all, an obvious absurdity.[113] The court's thinking goes as follows: a pen register (or its digital counterpart) is the mechanism by which law enforcement ascertains the cell site being activated by the target phone, and if a pen register cannot be involved in ascertaining the cell site, then Congress has forbidden law enforcement from using a very powerful tool without explicitly saying so.[114] Although the *S.D.N.Y. I* court found the "idea of combining some [statutory] mechanism with as yet undetermined features of [electronic privacy law] . . . an unattractive choice," it saw no other alternative but to accept the hybrid theory.[115]

---

[107] *See supra* text accompanying notes 75-83.

[108] *See supra* text accompanying notes 82-83; *see also Texas I*, 396 F. Supp. 2d at 759 n.16.

[109] *See supra* note 72.

[110] *See supra* text accompanying notes 82-83.

[111] *S.D.N.Y. I*, 405 F. Supp. 2d at 443-44.

[112] *Id.* at 441-42.

[113] *Id.*

[114] *Id.* at 441.

[115] *Id.* at 443-44.

The court in *S.D.N.Y. I* provided a plausible reading of the language in the relevant statutes, yet, as the opinion itself indicates, "the plain meaning of the words" of an ambiguous statute is not a strong foundation upon which to ground a statutory construction.[116] Because *S.D.N.Y. I* and those opinions adopting its reasoning made little use of the other tools of statutory construction, and completely ignored the policy implications of the hybrid theory, its validity remains questionable. Furthermore, the cases upholding the hybrid theory do very little to explain why privacy advocates' theory is unattractive. At most, the courts accepting the government's theory point to the limited precision with which law enforcement can track an individual, using the crudest form of cell location data.[117] The implication appears to be that, because certain types of cell location data do not permit the tracking of a target with the same precision as a conventional tracking device, the analogy, and the privacy advocates' argument, must fail.[118]

Whereas the hybrid theory relies almost entirely on a tenuous but plausible interpretation of several statutory sections regulating electronic surveillance, the alternative theory, which analogizes cell location data to the data derivable from a conventional tracking device, provides a cogent textual analysis, and, more importantly, situates that analysis in the overall structure of electronic surveillance law.

B. Cases Rejecting the Hybrid Theory

The line of cases that rejects the hybrid theory and analogizes cell location data to the data taken from a traditional tracking device has provided a thorough critique of the hybrid theory and offered its own interpretation of the relevant statutes.[119] The courts falling into this camp have grounded their decisions in a reading of the statutory texts and their legislative history that is contrary to the one provided by the hybrid theory, and, more importantly, in a structural argument that considers the framework of the ECPA as a

---

[116] *S.D.N.Y. I*, 405 F. Supp. 2d at 438.

[117] *See id.* at 437-38. For a discussion of cell location data, see *supra* notes 31-36 and accompanying text.

[118] For a more complete discussion of this point, see *infra* text accompanying notes 160-171.

[119] *See, e.g.*, *Texas III*, 441 F. Supp. 2d at 827-37; *E.D.N.Y. II*, 396 F. Supp. 2d at 305-08.

whole.[120] In seeking congruence with the basic design of the ECPA, these cases produce a more coherent interpretation of the ambiguous texts than does the 'plain meaning' approach taken by hybrid theory advocates. The overall soundness of this holistic approach is evidenced by the fact that the cases adopting it are by far the majority.[121] Yet despite an increasingly sophisticated and powerful critique of the hybrid theory, the hybrid's resilience was demonstrated in October of 2006, when a district judge in the Southern District of New York joined the hybrid camp.[122] The following is a discussion of the majority line of cases, which supplies various critiques of the hybrid theory and advances a more coherent alternative.

In light of the pervasive ambiguity in the statutes relied upon by the two competing theories (none of them actually mentions locating or tracking cellular phones by their transmissions), it should come as no surprise that the majority line of cases can also claim support for its analysis in the text of the relevant statutes.[123] The textual support for the 'tracking device theory' is quite sound: it is indisputable that cell phones "permit the tracking of the movement of a person or thing."[124] Courts accepting this position have also buttressed their holdings by referencing legislative history which is—admittedly—just as ambiguous as the statutes themselves.[125] Perhaps most importantly, the majority line of cases has produced a powerful critique of the hybrid theory. The following is a discussion of the hybrid theory's shortcomings

---

[120] *See Texas III*, at 827-37.

[121] In addition to the *E.D.N.Y I* and *II*; *Texas I* and *III*; *Maryland I* and *III*; and *E.D. Wis*. courts, district court opinions rejecting the hybrid theory have been handed down in the Western District of New York, *In re* Application of the United States of America for an Order Authorizing Installation and Use of a Pen Register (*W.D.N.Y.*), 415 F. Supp. 2d 211 (W.D.N.Y 2006); the District of Columbia, *In re* Application of the United States for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134 (D.D.C. 2006); *In re* Applications of the United States of America for Orders Authorizing Disclosure of Cell Cite Information, 2005 WL 3658531 (D.D.C. Oct. 26, 2005); the Southern District of New York, *In re* Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 2006 WL 468300, No. 06 CRIM. MISC. 01 (S.D.N.Y. Feb. 28, 2006); and in the District of Maryland, *In re* Application of the United States of America for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed] (*Maryland II*), 416 F. Supp. 2d 390 (D. Md. 2006).

[122] *S.D.N.Y. III*, 460 F. Supp. 2d at 454.

[123] *See, e.g.*, *Texas III*, 441 F. Supp. 2d at 832.

[124] *See supra* text accompanying notes 87-93; 18 U.S.C. 3117 (2006).

[125] *See Texas III*, 441 F. Supp. 2d at 832; *E.D.N.Y. I*, 384 F. Supp. 2d at 565-66.

identified in the opinions that have rejected it. These deficiencies are (1) the lack of any text instructing the combining of the essential statutes; (2) the period of years separating the enactment of the three critical statutes; (3) the hybrids' reliance on the Pen/Trap Statute as the exclusive source of authority for cell location data; (4) the theory's interpretation of the exception clause codified by CALEA; (5) the significance attached by the hybrid courts to the measure of precision with which a cell phone user can be tracked; (6) the lack of persuasive legislative history; (7) inconsistency with the basic design of the ECPA.[126]

1. The Lack of Internal Cross-Referencing

Courts rejecting the hybrid theory have questioned the validity of the theory's textual analysis. Several courts opposed to the hybrid theory have pointed out that none of the statutes that the government claims are meant to be combined even mentions another.[127] Although Congress' failure to explicitly instruct the necessary combination is not fatal to the hybrid theory, it is highly unusual for such a large grant of authority to law enforcement to receive no explicit mention from either the statutes alleged to grant such authority or from their legislative history. As the Supreme Court recently stated while rejecting an executive-branch claim to broad authority purported to be nestled in ambiguous statutory language, "Congress . . . does not, one might say, hide elephants in mouseholes."[128] To date, no court putting its imprimatur on the hybrid theory has offered an explanation for this anomaly.[129]

2. The Question of the Hybrid Theory's "Birthday"

One court noted that, in addition to the difficulty in determining how the ECPA brought the hybrid authority into being, there is the question of when that authority first existed.[130] The Pen/Trap Statute was enacted as part of the

---

[126] *See Texas III*, 441 F. Supp. 2d at 827-37; *W.D.N.Y.*, 415 F. Supp. 2d at 217-19, 218 nn.4-5.

[127] *See, e.g.*, *Texas I*, 396 F. Supp. 2d at 761. (There is one cross-reference, but it is the negative instruction found in 47 U.S.C. § 1002.)

[128] Gonzales v. Oregon, 546 U.S. 243, 267 (2006) (quoting Whitman v. Am. Trucking Ass'ns, Inc., 531 U.S. 457, 468 (2001)).

[129] *See Texas III*, 441 F. Supp. 2d at 835.

[130] *Texas I*, 396 F. Supp. 2d at 765.

ECPA in 1986.[131] CALEA, which contains the exception clause with its critically important phrase "solely pursuant to," was enacted in 1994. The USA PATRIOT Act, which purportedly expanded the scope of the Pen/Trap Statute to cover registration data, was not passed until 2001.[132] Given this timeline, accepting the hybrid theory requires accepting that in 1994 CALEA permitted the Pen/Trap Statute (in conjunction with the SCA) to access cell location data, even though cell phones were not in widespread use and even though the Pen/Trap Statute did not authorize the police to engage in meaningful surveillance of cell location data.[133] As with the lack of internal cross-referencing, hybrid theory proponents have not made an effort to explain this glitch.[134]

3. The Pen/Trap Statute as the Exclusive Source for Cell Location Authority

One of the assertions made by the leading case accepting the hybrid theory is that the Pen/Trap Statute is the *only* possible source of authority by which law enforcement can access cell location data.[135] The faulty syllogism that produces this conclusion runs as follows: Cell location data is "signaling information" within the meaning of the Pen/Trap Statute and therefore accessible via a pen register. The Pen/Trap Statute states that "no person may install or use a pen register . . . without first obtaining a court order under [the authority granted by the Pen/Trap Statute]."[136] Because only a pen register can provide the government with "signaling information," it must be that an order for a pen register is a necessary component of any court order providing cell location data.[137] If this were true, it would greatly undermine the tracking theory because it would mean that "[a warrant issued pursuant to probable cause] cannot by [itself] provide authority

---

131 Pub. L. No. 103-414, Title I, § 103.

132 *Id.*

133 *See id.* (arguing the converse, that is, if cell location data were already covered by the Pen/Trap Statute, then the 2001 amendment was unnecessary). *But see supra* note 64 and accompanying text (noting that the government has argued explicitly that the USA PATRIOT Act added "signaling information" so as to include cell location data).

134 *See Texas III*, 441 F. Supp. 2d at 835.

135 *S.D.N.Y. I*, 405 F. Supp. 2d at 441.

136 *Id.* at 441; *see also* 18 U.S.C. §§ 3123, 3127(3) (2006).

137 *S.D.N.Y .I*, 405 F. Supp. 2d at 441.

for the Government's application because any warrant . . . must necessarily authorize the installation of a 'pen register.'"[138] In other words, given that only a pen register has the technological capability to obtain cell location data, to hold that an order for a pen register is insufficient legal authority to obtain the same information would mean that the government cannot obtain cell location data by any means. Such a result, the court rightfully concludes, cannot be squared with the clear intention of the relevant statutes.[139]

Another court responded to this argument, vigorously attacking the syllogism.[140] This second court stated that if the hybrid theory is correct in this regard, then the "pen/trap standard is not only a threshold, but also a ceiling," an equally bizarre result.[141] It then demonstrated that the hybrid court's conclusion contravenes some of the basic principles of the ECPA. The court stated, "One feature of ECPA is that through use of greater legal process officials can gain access to any information that they could obtain with lesser process."[142] Even more convincingly, the court cites the manual published by the Department of Justice's Computer Crime and Intellectual Property Section for the proposition that "a § 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a § 2703(d) order can compel (and then some.)"[143] If still more authority were required, the court critiquing the syllogism discussed a Supreme Court opinion written before the enactment of the ECPA, which specifically stated that a warrant could obtain the type of information later covered by the Pen/Trap Statute.[144]

There is another serious problem with trying to argue that a pen register is the exclusive method for accessing cell location data. First, it is not exactly accurate to state that a pen register is the device that captures cell location data. The court in *S.D.N.Y. I* itself noted that, at least in its own district, a "pen register" no longer refers to a physical device that agents

---

[138] *S.D.N.Y .I*, 405 F. Supp. 2d at 441.

[139] *Id.* at 441-42.

[140] *Texas III*, 441 F. Supp. 2d at 829-32.

[141] *Id.* at 829.

[142] *Id.* (quoting J. CARR & P. BELLIA, *supra* note 51, § 4:77, at 4-193 internal quotes omitted).

[143] *Id.*

[144] *Id.* at 830 (discussing United States v. N.Y. Tel. Co., 434 U.S. 159 (1977), and noting that it has not been overruled in light of the ECPA).

install on a subscriber's line.[145] On the contrary, data from a "pen register" now exists in the form of a digital record, which the phone company provides to law enforcement after receiving a court order.[146] The court noted that in the context of digital telephony, "[t]he Government has properly assumed that, despite this change in technology, it is bound to follow the Pen Register Statute to obtain information otherwise covered by the statute."[147] The court lost itself in its own fictions when it asserted that a pen register is the only "device" by which the government can obtain cell location data.[148] By defeating the argument that only a pen register can access cell location data, the hybrid theory's detractors open the possibility that a warrant issued in accordance with 18 U.S.C. § 3117 is the appropriate form of authority.

4. Reading "Solely Pursuant to" in 47 U.S.C. § 1002

Closely tied to its reading of the Pen/Trap Statute, the court in *S.D.N.Y. I* read the exception clause in 47 U.S.C. § 1002 to mean that an order for a pen register was a necessary component of an order for cell location data.[149] The court stated that "'[s]olely' means 'without another' or 'to the exclusion of all else.' 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."[150] In drawing that conclusion, the court mistook one possible meaning for the only available meaning.

The court in *Texas III* responded by asking us to "[c]onsider the statement 'A barrel of oil cannot be purchased *solely* with a $5 bill.'"[151] The logic employed by the New York court would lead to the conclusion that no amount of currency and no property offered as barter could secure the purchase of a barrel of oil unless it included or was accompanied by a $5 bill. The court in *Texas III* reached a different conclusion—one that is amply supported by the design of the ECPA: although "some amount of legal process" is necessary to obtain cell

---

145 *S.D.N.Y. I*, 405 F. Supp. 2d at 438 n.1.

146 *Id.*

147 *Id.*

148 *See id.* at 441.

149 *Id.* at 440-44.

150 *Id.* at 442 (internal citations omitted) (alterations and emphasis in original).

151 *Texas III*, 441 F. Supp. 2d at 833.

location data, the authority granted by the Pen/Trap Statute is not enough.[152] The Texas court's barrel of oil example demonstrates that the exception clause can be read to mean that greater legal process could 'purchase' greater powers of surveillance. The court thereby demonstrated that the hybrid theory's essential claim—that the exception clause requires pen register authority for law enforcement to access cell location data—is not the only possible reading of that section.

Another odd result produced by reading the exception clause as the hybrid theory requires was manifested in a case from the Southern District of West Virginia ("*West Virginia Opinion*").[153] That court noted that the exception clause prohibits a pen register from disclosing the physical location of the *subscriber* to a telephone service.[154] Because the target of the police surveillance in the *West Virginia Opinion* was not the subscriber to the phone company's service, but rather was using another person's phone, the court held that the phone user's cell location data was accessible on the minimal showing of certified relevance.[155] This is problematic for three reasons. The first is obvious. By accepting the hybrid theory's initial premise, that cell location data is accessible via a pen register, a court is forced to conclude that there is only minimal procedural protection available for cell phone users who are not the service subscriber. If this were true, it would mean that an individual's privacy interest in being free from having the government track his or her movements is created by contracting for cellular telephone service. The second problem compounds the first. Under the "certified relevance" standard, a district court could not question law enforcement's assertion that the target of the surveillance is not the service subscriber.[156] The *West Virginia Opinion* exemplified this exact

---

[152] *Texas III*, 441 F. Supp. 2d at 833; *see also supra* notes 40-41 and accompanying text.

[153] *In re* Application of the United States of America 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 (*W. Va. Opinion*), 415 F. Supp. 2d 663 (S.D. W. Va. 2006).

[154] *Id.* at 665-66; s*ee also* 47 U.S.C. § 1002 (2006).

[155] *W. Va. Opinion*, 415 F. Supp. 2d at 665-66. The court did note that it would not follow the hybrid theory where a subscriber's location was sought. In drawing its distinction, it accepted the premise that a pen register is the proper source of cell location data, but rejected in dicta the hybrid theory's applicability to service subscribers.

[156] *See Texas I*, 396 F. Supp. 2d at 753 (stating that when considering an application where the government is held to the evidentiary burden of certified relevance, "the judge need not—and, indeed, cannot—independently assess the factual

concern when it stated "[t]he United States certifies that the fugitive is using another person's cellphone."[157] The practical effect of such a rule would permit the government to engage in warrantless, real-time tracking of individuals anytime a government agent represents that a suspect is carrying the cell phone of another.

It is no less invasive of one's privacy to have one's movements tracked when carrying someone else's cell phone than it is to be tracked with one's own cell phone; this is a necessary result of accepting the hybrid theory and is inconsistent with the feature of the ECPA that calibrates the amount of required legal process to the degree of intrusion into one's privacy.[158] Moreover, if the hybrid interpretation of the ECPA is the correct one, then the statute is unconstitutional to the extent it permits the government to monitor cell phone users' movements within their homes but without a warrant.[159]

5. The Precision of Tracking Made Possible by Cell Location Data

Cell location data can be grouped into various types, some permitting more precise tracking than others, and some involving a different amount of voluntarism on the part of the user.[160] For instance, in the first published opinion to reject the hybrid theory, the government requested prospective cell location data, but only regarding the individual cell site activated by the target phone.[161] In an application before a different court, the government requested prospective data, but from multiple cell sites, susceptible to triangulation, as well as the signal strength data from each cell site.[162] The government application before that magistrate requested the most precise data set possible from conventional wireless telephony.[163] Had the request been granted, it would have allowed ongoing, real-

---

predicate for the government officials' certification") (quoting CARR & BELLIA, *supra* note 51, § 1:26, at 1-25); s*ee also supra* text accompanying notes 65-70.

157 *W. Va. Opinion*, 415 F. Supp. 2d at 664.

158 *See supra* note 70.

159 *See supra* note 46 and accompanying text.

160 *See supra* note 45.

161 *E.D.N.Y. I*, 384 F. Supp. 2d at 563; *see also E.D.N.Y. II*, 396 F. Supp. 2d at 295.

162 *Texas I*, 396 F. Supp. 2d at 749; *see also supra* text accompanying notes 31-38.

163 *See supra* text accompanying notes 41-42.

time tracking of the subject phone with a high degree of precision.[164]

By contrast, in the leading case to accept the hybrid theory, the government sought, on a prospective basis, cell site data and facing data generated at the beginning and end of calls, but not triangulation data, signal strength data, or automatically generated registration data.[165] The split among the courts cannot be explained by the differences in the data sets requested by law enforcement in the various cases. Pointing to the differences in precision made possible by the data is at best a partial explanation for the split, evidenced by the split between the Eastern District of New York and Magistrate Judge Gorenstein's opinion in *S.D.N.Y. I*. The opinions handed down in the Eastern District denied a government application for less invasive data than the application which was granted in *S.D.N.Y. I*.[166]

Moreover, if the cases accepting the hybrid theory are best understood as permitting the warrantless locating or tracking of cell phones when that surveillance is conducted with limited precision, then their deciding rationale is unsound; it is certainly not rooted in the text of the ECPA.[167] As one court that rejected the hybrid theory has noted, the federal statute defining tracking devices does not include a precision requirement in its definition.[168] Yet, every one of the cases that has accepted the hybrid theory has limited its holding to cell location data that reveals only generally the location of its target.[169] Those courts' reluctance to grant law enforcement the full measure of surveillance capability that the hybrid theory authorizes is understandable, but there is no principled basis for limiting the theory's reach in this way.[170] The hybrid courts' unease suggests that, however convincingly the hybrid theory might account for the text of the relevant statutes, what it proposes is just bad policy.

---

[164] It is unclear exactly how precisely the government would have been able to track the phone; that can never be known unless the concentration and arrangement of cell towers activated by the phone is also known. *See supra* text accompanying notes 20-38.

[165] *S.D.N.Y. I*, 405 F. Supp. 2d at 437; *see also* Dempsey, *supra* note 1, at 537.

[166] *Compare E.D.N.Y. II*, 396 F. Supp. 2d at 295-96, *with S.D.N.Y. I*, 405 F. Supp. 2d at 437-38 (denying the same application on rehearing).

[167] S*ee supra* text accompanying notes 89-93.

[168] *Texas I*, 396 F. Supp. 2d at 753.

[169] *See Texas III*, 441 F. Supp. 2d at 827.

[170] *See W.D.N.Y.*, 415 F. Supp. 2d at 218 n.5.

6. The Lack of Persuasive Legislative History

Both sides of the debate claim to have found support in the language of the legislative histories of the various statutes involved in the debate.[171] Although there is a significant amount of skepticism regarding the value of legislative history, Justice Scalia being its foremost critic, the history of the statutes relevant to the present debate has been the topic of constant skirmishing between the two camps in the controversy.[172] Hybrid theorists offer the legislative history of the USA PATRIOT Act to reinforce their argument's essential claim that "signaling information" includes "cell location data."[173] The quoted history supports the assertion that the Pen/Trap Statute authorizes the use of pen registers to capture data from cellular phones in addition to other electronic communication media, such as email, but it does not shed much light on whether cell location data should be construed as "signaling information." Because this is the only legislative history that putatively supports the argument that cell location data is "signaling information," this appeal to the statute's history is hardly convincing. One court that rejected the hybrid theory likely had this point in mind when it declared that "[n]othing in the admittedly abbreviated legislative history of the PATRIOT Act suggests this new definition would extend the reach of the Pen/Trap Statute to cell phone tracking."[174]

The hybrid proponents' most convincing use of legislative history regards their interpretation of the exception clause, codified as part of CALEA.[175] Hybrid proponents point to the first round of testimony given before Congress by former FBI director Louis Freeh, who was appearing to urge the enactment of CALEA.[176] He stated, "Even when such generalized location information . . . is obtained from communications service providers, *court orders* or *subpoenas*

---

[171] *See, e.g.*, *S.D.N.Y. I*, 405 F. Supp. 2d at 439-41, 443; *Texas I*, 396 F. Supp. 2d at 752 n.7, 753-54, 758, 761-65.

[172] *See generally* ANTONIN SCALIA, A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW (1997).

[173] *See S.D.N.Y. I*, 405 F. Supp. 2d at 438-39; *see also supra* text accompanying notes 101-104.

[174] *Texas I*, 396 F. Supp. 2d at 761.

[175] *S.D.N.Y. I*, 405 F. Supp. 2d at 442-43.

[176] *See id.* at 443.

are required and are obtained."[177] At first blush, the FBI director's use of the words "court orders or subpoenas" and not "warrants issued pursuant to probable cause" seems to bolster the hybrid argument. This conclusion is significantly undermined if Director Freeh was only referring to historical data or to a person's actual, physical address (readily identifiable in the erstwhile era of wireline telephony, the predominant mode of telephony at the time Freeh made these statements) when he used the term "generalized location information."[178] Perhaps more to the point, the leading opinion to adopt the hybrid theory only used the Freeh statement to support its argument that the exception clause contained in CALEA can't be read to "bar[] law enforcement agencies from obtaining cell site information entirely," a point not seriously contended in the opinions rejecting the hybrid theory.[179]

Courts rejecting the hybrid theory have also relied on the statements Freeh made before Congress. In one portion of testimony, he stated that the purpose of CALEA was to "maintain technological capabilities commensurate with existing statutory authority."[180] Freeh's concern was that, as digital telephony—both wireless and wireline—came to replace traditional analogue telephony, the existing statutes authorizing the compelled cooperation of phone companies would be eroded, and that law enforcement would lose the ability to "install" pen registers and wiretaps.[181] In an attempt to allay the concerns of privacy advocates, Freeh stated that CALEA "ensures the maintenance of the status quo," and that "the legislation does not enlarge or reduce the government's authority to lawfully conduct court-ordered electronic surveillance."[182] This use of legislative history, while it tends to strengthen the argument against the hybrid theory, is ultimately inconclusive. Relying on this testimony to demonstrate that CALEA was not meant to authorize the use

---

[177] *S.D.N.Y. I*, 405 F. Supp. 2d at 443 (quoting *Police Access to Advanced Communications Systems: Hearing Before the Subcomm. on Technology and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 2d Session (1994) (statement of Louis Freeh, Director of the FBI) (emphasis added).

[178] *See id.*

[179] *Id.*; *see infra* text accompanying notes 181-184.

[180] *Wiretapping Access: Hearing Before the Subcomm. on Telecommunications and Finance of the H. Comm. on Energy and Commerce*, 103d Cong. (1994).

[181] *Id.*

[182] *Id.*

of pen registers to track cell phones simply begs the question of whether such use of pen registers is an expansion of the government's pre-digital powers of surveillance or simply maintenance of the status quo.

The fact that both sides of this debate claim the support of the same legislative history is not surprising; nor is the fact that neither snippet of Freeh's testimony definitively answers the question of what the critical terms mean. Justice Scalia has argued that the law is manifested by the "objective indication of the words [of a statute], rather than the intent of the legislature."[183] He points out that the attempt to discern congressional intent from legislative history is flawed in at least three related ways. First, it invites judges to implement their own policy preferences under the guise of legislative intent.[184] Second, to suppose an actual intent shared by a majority of Congress behind any given statute (to say nothing of such statutory minutiae as is involved in the present controversy) is to indulge an enormous fiction.[185] Indeed, it is difficult to imagine that a majority of the members of Congress actually thought about and shared an opinion as to how the terms "signaling information" or "solely pursuant to" should apply to cell location data. Finally, the sheer volume of documentation produced in passing new laws means that litigators and judges turning to legislative history will find "something for everybody."[186] Rather than asking what Congress intended but failed to express, the proper inquiry into legislative intent asks what Congress' intentions were, as objectively manifested in the words they actually used.[187] The reasoning in some of the cell location cases exemplify the problems inherent in relying on legislative history, and validate Justice Scalia's critiques of the practice.[188]

The theory of textualism advanced by Justice Scalia offers an alternative interpretive technique for resolving ambiguities such as the ones at the heart of the present controversy. It urges that words have a limited range of possible meanings and seeks to determine the most reasonable

---

183 SCALIA, *supra* note 172, at 29.

184 *Id.* at 30-31.

185 *Id.* at 31-32.

186 *Id.* at 36.

187 *Id.* at 16-17

188 *See supra* text accompanying notes 171-172.

interpretation of the words themselves.[189] While textualism does not resort to legislative history, it does consider the context in which ambiguous words are situated to determine their meaning.[190] Whatever may be said of textualism generally, relying on the "'objectified' intent—the intent that a reasonable person would gather from the text of the law, placed alongside the remainder of the *corpus juris*," produces a decisive insight in the cell location cases.[191] Courts accepting the hybrid theory have analyzed the critical statutory sections only in isolation from the body of federal electronic surveillance law. Those courts' conclusions, though credible on their own terms, are inconsistent with the basic design of the ECPA and counter to the policies embodied in that statute.[192]

7. The Structural Inconsistencies Created by the Hybrid Theory

Considering the texts of the three statutory provisions essential to the hybrid theory within the context of the ECPA's regulatory scheme fatally undermines the government's argument. As noted in one prominent opinion rejecting the hybrid theory, the provisions of the ECPA that explicitly govern access to forms of prospective data contain sealing requirements and time limits.[193] The SCA contains none.[194] The court reasoned that these features of the Pen/Trap Statute and the SCA indicate that they were tailored to different purposes and meant to operate separately rather than in tandem.[195] Another court noted that accepting the hybrid theory requires accepting that the "two statutes together accomplish what neither can alone."[196] This is especially odd given that the statutory ingredients in the hybrid theory were enacted over a

---

[189] SCALIA, *supra* note 172, at 24.

[190] *See id.* at 20-21, 23-24.

[191] *Id.* at 17 (citations omitted).

[192] *See Texas III*, 441 F. Supp. 2d at 829; *see also* Kerr, *supra* note 70, at 608-09.

[193] *See Texas III*, 441 F. Supp. 2d at 833-36 (noting that wiretaps, which are inherently prospective, can be authorized for a maximum of thirty days at a time, that pen/trap authorizations expire after sixty days, and that both wiretap and pen/trap orders are automatically sealed while orders under the SCA trigger none of these privacy protections).

[194] *Id.* at 833.

[195] *Id.* at 835.

[196] *E.D.N.Y. II*, 396 F. Supp. 2d at 316.

fifteen-year period, and that, with one exception, they do not cross-reference one another.[197]

Another anomaly that the hybrid theory produces in the structural coherence of the ECPA was noted by Magistrate Judge Smith in the Southern District of Texas: the warrant requirement for a tracking device would be redundant if law enforcement can effectively track an individual with a cell phone.[198] While the court's opinion may have overstated the case by suggesting that law enforcement could simply install cell phones on people's cars instead of actual tracking devices (thereby obviating the need for a warrant), the point is well-taken that given the ubiquity of cell phone usage, a tracking device would seldom be necessary if the cell phone could perform a tracking function while not requiring a warrant.[199]

Finally, it has been observed that the ECPA requires greater legal process in order for the government to access data that is more invasive of an individual's privacy.[200] As part of this basic design, the authority for pen registers is quite easy to exercise, representing a judgment on the part of Congress that phone users have a limited privacy interest in the record of phone calls they have made.[201] At the other end of the ECPA's spectrum is the authority for wiretapping, requiring what Orin Kerr has called the "'super' search warrant."[202] Just below the super warrant in the hierarchy of legal process is the warrant issued pursuant to probable cause, the normal form of authorization for installing a tracking device.[203] The fact that a warrant is normally required to track an individual's movement suggests that a significant privacy interest is invaded when law enforcement engages in this type of surveillance.

One potential response from advocates of the hybrid theory maintains that traditional pen registers revealed the location of phone users at the time they were on the phone, usually in their homes and offices, the very places that the Supreme Court has held deserve the greatest privacy

---

[197] *Texas I*, 396 F. Supp. 2d at 764-66. The one cross-reference is a limiting reference, located within the exception clause of § 1002. *Id.* at 764; *see also supra* notes 130-134 and accompanying text.

[198] *Texas I*, 396 F. Supp. 2d at 756.

[199] *See id.*

[200] Kerr, *supra* note 70, at 620-21.

[201] *See supra* text accompanying notes 65-70.

[202] Kerr, *supra* note 70, at 620.

[203] *Id.*; *see also supra* note 51.

protections. That this information was and is accessible without a warrant suggests that the ECPA also permits cell location data to be accessible without a warrant, even when it reveals the phone user is inside his or her home. This argument fails to acknowledge that technology which permits the real-time tracking of individuals is clearly more powerful and more invasive than technology that merely determines a person was at home or in their office at the time they made a phone call. The differences are important. First, the cell phone service subscriber is typically the exclusive user of her cell phone, whereas ten or fifteen years ago, an entire household shared a single phone line. This development increases the certainty—to nearly one hundred percent—that the government can locate an individual by locating a particular phone. Second, pen registers on a landline could disclose the person's whereabouts only at the time they were making a call, as opposed to the constant monitoring that cell location data makes available. This is not a quantitative but a qualitative difference. The difference is so great that it makes cell location data functionally indistinguishable from data derived from a tracking device and completely unlike the list of dialed numbers derivable from a pen register. Under the ECPA, whenever the government seeks a greater intrusion into a person's privacy, greater legal process is required.[204] This observation suggests that emerging forms of electronic surveillance—such as cell phone monitoring—should be regulated according to function and not according to strained linguistic analyses.

The previous discussion recounted the various critiques of the hybrid theory offered by the majority line of cases. Of all the conceptual problems posed by the government's theory, the most serious is the observation that the constituent sections of the ECPA be interpreted with regard to their function.[205] The hybrid theory apparently has no answer to this insight; the theory's best defense is a brittle insistence upon one very particular reading of the relevant statutory sections. This reading studiously ignores the fact that the government monitors the movements of a person or thing when it accesses prospective cell location data, regardless of whether that data is called "signaling information," "subscriber records" or "data

---

[204] Kerr, *supra* note 70, at 620-21.

[205] *Id.*

from a tracking device." Even the cases accepting the hybrid theory have limited its impact in a manner that suggests its central premise—that law enforcement can use electronic surveillance to monitor a person's whereabouts with a minimal amount of judicial oversight—is inconsistent with the policies behind the ECPA.[206]

V. CONCLUSION

The debate over cell location data reflects a general truth about the current state of electronic media law—it is outdated and falling further behind.[207] The proliferation of Internet traffic and technological advances in such areas as data storage and wireless telephony that have taken place in the last ten years have profoundly changed the way human communities exchange, store, process, and commodify information.[208] The startling speed of these changes made it inevitable that the laws regulating the flow of information would lag behind.[209] The Internet, now the most important information medium for individuals, corporations and government, is regulated—to the extent it is regulated at all—by laws modeled on telephonic communications media.[210] The awkward fit between those laws and their new subject has not gone unnoticed.[211] In the context of electronic privacy, courts have been left to apply a regulatory framework designed for the previous epoch. The controversy over cell location data takes place in one small corner of this broad frontier. Striking the right balance between the values to which we as a free people are committed and the need to protect ourselves from domestic and foreign threats is perhaps the most important task facing our lawmakers.

It is by no means clear where that balance is to be found, but in our institutions are policies and practices that have served us throughout our history and that continue to find application to contemporary problems. Foremost among them is the doctrine of the separation of powers. Because each

---

206 *See supra* note 70 and accompanying text.

207 *See* Lockwood, *supra* note 8, at 317.

208 Dempsey, *supra* note 1, at 516-18, 529-33.

209 *See* Susan P. Crawford, *The Ambulance, the Squad Car & the Internet*, 21 BERKELEY TECH. L.J. 873, 876 (2006).

210 *Id.* at 889-94.

211 *See* Lockwood, *supra* note 8, at 317.

branch of our government is given a limited sphere of influence, each serves as a check on the power of the others in order to preserve the rights and liberties of the sovereign American people.[212] Updating the Executive's tool kit in its struggle against both the common criminal and sophisticated enemies of the state is an important task, but the judiciary has, since the time of the founding, provided the check that protects Americans' privacy from government overreaching.[213] Although the Supreme Court has not extended the Fourth Amendment's warrant requirement to many forms of electronic surveillance,[214] Congress has legislated in this area and imposed greater privacy protections than are required by the Constitution.[215] The following are some suggestions for amendments to the existing statutes that would explicitly create a role for judicial oversight regarding cell location data.

1. Clarifying the Scope of the Pen/Trap Statute. The first step in the hybrid theory posits that cell location data is accessible via the device (or process) that creates a record of all numbers dialed by the target phone and that the government may therefore use the legal authorization for such a record to locate and track individuals.[216] Because of the breadth of its terms, the Pen/Trap Statute's application to cell location data is at least plausible.[217] Perhaps Congress used such broad terms out of a concern that pen registers would be made obsolete by the change from analogue to digital and from wireline to wireless telephony. Or perhaps they were concerned that unforeseen technological changes would quickly render the new amendments obsolete. Such an interpretation of the Pen/Trap Statute is at least as plausible as the interpretation of the one advanced by the hybrid theory.

Congress should amend 18 U.S.C. § 3127(3) by inserting language such as "nor shall such information include any data that would reveal the physical location of the phone user (except to the extent that the location may be determined from a wireline-connected telephone number)" after the language in that subsection that prohibits intercepting the content of

---

[212] Erwin Chemerinsky, *The Assault on the Constitution: Executive Power and the War on Terrorism*, 40 U.C. DAVIS L. REV. 1, 4-5 (2006).

[213] *See* Freytag v. Comm'r, 501 U.S. 868, 870 (1991) (stating that the separation of powers is the "central guarantee of a just government").

[214] *See supra* notes 44-45 and accompanying text.

[215] *See supra* note 47 and accompanying text.

[216] *See supra* notes 61-65 and accompanying text.

[217] *See supra* notes 80-83 and accompanying text.

communications.[218] This amendment would preclude the use of pen registers to track cell phones, leaving a warrant issued under the authority of 18 U.S.C. § 3117 as the appropriate form of authority for compelling the disclosure of cell location data.[219] Such an amendment would also leave intact the "status quo" to which Director Freeh referred in his testimony before Congress—law enforcement agencies could still access pen register data without learning anything about a cell phone user's location.[220]

2. Rewording the "Exception Clause." Another possible amendment would more clearly define Congress' intention behind the phrase "solely pursuant to" in the exception clause of 47 U.S.C. § 1002. If Congress wanted to prohibit the warrantless tracking of cell phones, this section could be amended simply by excising the word "solely." Such change would end any speculation that this part of CALEA is an implicit instruction to combine two statutes conveying different forms of authority so as to authorize a third, remarkably more powerful form of surveillance. As it reads now, the most natural reading of the phrase "solely pursuant to" supports the hybrid theorists' textual arguments.[221] The term "solely" does indeed suggest the meaning "with another," even if it is not (as some courts have held) the only possible meaning.[222] In the absence of some text specifying what that other authority should be, it is reasonable to expect law enforcement to select its preferred form of authority and equally reasonable to expect courts to be divided by the questions raised by government applications for cell location data. At the very least, if Congress does intend for § 1002 to act as the bridge between the Pen/Trap Statute and the SCA, they should amend the section by replacing the term "subscriber" with "user" in order to avoid the bizarre result in the *West Virginia Opinion*.[223]

---

[218] *See* 18 U.S.C § 3127(3) (2006).

[219] *See supra* note 51.

[220] *See supra* notes 175-182 and accompanying text. Note also that at least one other commentator has suggested amending the Pen/Trap Statute, albeit in a slightly different fashion. Rickey G. Glover, Note, *A Probable Nightmare: Lifting the Fog from the Cellular Surveillance Statutory Catastrophe*, 41 VAL. U. L. REV. 1543, 1581-83 (2007). Regardless of the actual wording, any amendment to the Pen/Trap Statute should explicitly prohibit the disclosure of an individual's location via Pen/Trap authority.

[221] *See supra* notes 110-115 and accompanying text.

[222] *See supra* notes 149-159 and accompanying text.

[223] *See supra* notes 153-159 and accompanying text.

3. Amending the Stored Communications Act. Congress could amend the SCA section that completes the hybrid theory in much the same way as the Pen/Trap Statute if it wanted to prohibit warrantless cell phone tracking.[224] The phrase "or any information regarding the physical location of the user of such service" could be inserted into the parentheses excepting the contents of electronic communications from the aegis of 18 U.S.C. § 2703(c)(1). Such an amendment would be a good idea regardless of whether the other amendments are made. As one commentator noted, the SCA deals with stored communications, but is susceptible to the argument that a communication is "stored" the moment its existence is recorded by phone company computers.[225] The success of such an argument would turn the statute—with its focus on making records stored in phone company computers accessible to law enforcement—into a prospective grant of authority to note calls as they take place, provided they are "stored" for some trivial amount of time before being disclosed.[226] If the record of cell towers activated by cell phone transmissions is cognizable as "other information," then the government could, in theory, achieve the same result under the SCA that it sought under the hybrid theory.[227] An amendment that clearly forbade the release of a phone user's physical location would prevent this crafty argument from authorizing cell phone tracking.

Whether or not Congress would want to prohibit warrantless cell phone tracking is unclear. The legislature could, of course, explicitly authorize the government to conduct warrantless cell phone tracking. As long as the target phone is never carried into an area where its user enjoys a reasonable expectation of privacy, there would be no constitutional defect in the application of such a statute.[228] This Note has argued, however, that such a change in the country's electronic surveillance regime would be a regression. Congress has promulgated a scheme that requires a degree of judicial oversight, commensurate with the inherent invasion of privacy, by requiring the government to obtain an order authorizing

---

[224] *See* 18 U.S.C. § 2703(c)(1) (2006).

[225] Dempsey, *supra* note 1, at 539.

[226] *See id.* By simply keeping a record in their computers for five or ten minutes, phone companies would convert what is essentially real-time data into "stored" communications. This information would then be disclosed to the government on an ongoing basis.

[227] *See* 18 U.S.C. § 2703(c)(1) (2006).

[228] *See supra* note 46 and accompanying text.

such surveillance.[229] This is good policy, respecting as it does the tension between liberty and order that must always exist where a people choose to live freely in a perilous world.

The hybrid theory presents a textual analysis of federal electronic surveillance laws that is plausible on its own terms, but fails to explain why cell location data is *better* analyzed as pen register data than as data from a tracking device. It cannot account for the regulatory design of the ECPA, discernible in the graduated levels of judicial oversight required for more invasive forms of surveillance[230] nor for the fact that once the government can ascertain an individual's general location with cell site data, there is no principled way to prevent the government from using more sophisticated data sets to track individuals in real time and with a high degree of precision.[231] The alternative theory, by contrast, can account for the language in the relevant statutes, support the policies embodied in the ECPA, and retain a meaningful role for the judiciary in determining, *ex ante*, how much surveillance the executive branch may lawfully conduct.[232]

Law enforcement's ingenuity is on display in the cell location cases, and there is cause for satisfaction in the idea that police agencies are adapting their techniques to take advantage of emerging technologies. Yet, if we are to preserve the right to be free from pervasive governmental intrusion in our private lives, we must be careful how much deference we accord to law enforcement's claims of authority.[233] Treating cell location data as analogous to data from a tracking device imposes a neutral and detached decision-maker between the police, "engaged in the often competitive enterprise of ferreting out crime," and private citizens.[234] A careful reading of the relevant statutes demonstrates that this conclusion is not only preferable, it is the one required by the will of Congress.

Timothy Stapleton[†]

---

[229] CARR & BELLIA, *supra*, note 51, § 4:77, at p. 4-193.

[230] *Id.*

[231] *See supra* notes 167-170 and accompanying text.

[232] *See supra* Part IV.B.

[233] *See* Johnson v. United States, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.").

[234] *Id.*

[†] The author would like to thank Professors Susan Herman and Wendy Seltzer for their invaluable contributions to this Note.