FROM CELL TO SLAMMER: FLAWS OF THE HYBRID THEORY

Lisa M. Lindemenn*

This Note analyzes the flaws of a government-created "super statute." In an unprecedented form of statutory interpretation—known as the hybrid theory—the federal government combines the authority of two portions of the Electronic Communications Privacy Act to assert authority that does not exist under either portion alone. The government has repeatedly relied on this artificial authority to obtain court orders approving the use of wireless telephones as tracking devices, thus sidestepping the probable cause standard traditionally required for such an intrusive form of surveillance. When this surveillance identifies individuals inside their homes, Fourth Amendment concerns are implicated. Because the court orders routinely remain sealed even after surveillance is terminated, however, individuals are precluded from appealing the orders and remedying the potential constitutional violations. Moreover, even if individuals learn of the surveillance and bring claims against the government, those claims are likely to be dismissed on procedural grounds. The lack of opportunity for appellate courts to reach the issue means the government is essentially controlling the development of the law. This Note recognizes the need for legislative or, in the interim, judicial action to rectify that problem.

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2011. Thank you first to the Honorable Charles R. Pyle and his law clerk Lori Price for introducing me to the hybrid theory and for offering their invaluable insight. Thank you also to the editors of the *Arizona Law Review*, particularly Frances Sjoberg for her encouragement and guidance and the amazing team of Managing Editors for sticking with me through this process. Finally, thank you to my family for their support and to my husband Matt for his patience.

TABLE OF CONTENTS

INTRODUCTION

At the end of 2010, the wireless service industry reported over 300 million subscribers in the United States, which represents approximately 96% of the country's population.[1] At any time wireless telephones are turned on, irrespective of whether calls are being made or received, wireless providers record data known as "cell site location information."[2] As the name suggests, this information can be used to track the geographic location and movement of wireless telephones and, by extension, their users.[3] Recording of cell site location information has critical functions in modern society.[4] But as the number of

1. *Wireless Quick Facts: Year End Figures*, CTIA – THE WIRELESS ASS'N, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (Dec. 2010).

2. *See infra* Part I.A.

3. *See infra* Part I.B.

4. For example, using cell site location information to track a missing person's wireless telephone may help authorities recover the person. Ken Wallentine, *Cell Site Location Evidence: A New Frontier in Cyber-Investigation*, 2011 AMS. FOR EFFECTIVE L.

wireless telephone users continues to grow, the potential for Big Brother to track the location of virtually every person in the United States at any given time is becoming reality.[5] When the U.S. government seeks to obtain information regarding the location of particular wireless telephone users, there are unsettled statutory issues and privacy concerns.

Indeed, there is no law directly addressing the standard the government must meet to obtain cell site location information. And, to further complicate the issue, there are different types of cell site location information that, under existing statutes, probably should be subject to different standards. For instance, this Note will distinguish between "historical" and "real time," or prospective, cell site location information and will acknowledge different standards depending on which type of information the government seeks.[6]

Given the lack of congressional direction, the government asserts authority to obtain cell site location information from various statutes and combinations of statutes. Most troubling are the government's requests to obtain real time cell site location information—which, in practice, renders wireless telephones tracking devices—under a lesser standard than typically required for such intrusive forms of surveillance. As one scholar stated, routine judicial authorization of these requests without requiring the government to show probable cause is "a stunning revelation."[7]

To overcome the traditional probable cause requirement, the federal government employs a novel approach to statutory interpretation. In its so-called hybrid theory, the government combines the authority of the "Pen/Trap Statute"[8] with the authority of the Stored Communications Act (SCA)[9] to create a "super statute" with more expansive authority than either of the two statutes has alone.

Ample evidence suggests the government's creation of a super statute that provides greatly enhanced disclosure with a lower government burden is a flawed form of statutory interpretation with adverse consequences. Shielded by the system of ex parte applications and cases that remain sealed "until otherwise ordered by the court,"[10] the federal government essentially controls the development of the law from a judicial standpoint. As a survey of electronic surveillance orders issued by Houston magistrate judges shows, orders issued under seal overwhelmingly remain sealed even after the criminal investigations are closed.[11] Thus, unless the

---

ENFORCEMENT MONTHLY L.J. 401, 402.

5. *See id.*

6. Where necessary, the Note will also differentiate between information derived from single cell towers and information derived from multiple cell towers. For a discussion of how the information differs, see *infra* notes 51–53 and accompanying text.

7. Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 609 (2007).

8. 18 U.S.C. §§ 3121–3127 (2006 & Supp. 2009).

9. 18 U.S.C. §§ 2701–2712 (2006).

10. Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 FED. CTS. L. REV. 177, 209 (2009).

11. *Id.* at 209–10. The survey found that Houston magistrate judges issued 3886 orders for electronic surveillance under seal for the period between 1995 and 2007. In 2009, after the close of the criminal investigations, 99.8% of the orders remained sealed. *Id.*

surveillance is used as trial evidence, individuals may never know that their movements were monitored and have no opportunity to appeal orders signed under questionable legal authority.

In fact, since 2005, when a federal magistrate judge from the Eastern District of New York published the first opinion denying a government request for cell site location information,[12] district courts have split over whether to accept the government's asserted authorities.[13] While this split should make the issue a prime candidate for appellate review, in more than five years since it came to the attention of the legal world no case addressing the legal standard the government must meet to obtain *real time* cell site location information has reached a Circuit Court of Appeals.

The Third Circuit recently held that district courts have discretion to authorize disclosure of *historic* cell site location information upon the government meeting a standard lower than probable cause.[14] The government's choice to appeal that particular district court decision was undoubtedly calculated, however, as few other courts have held that the government is not entitled to *historic* cell site location information under a lesser standard.[15] Moreover, the government did not assert authority to obtain the historic location information using the hybrid

---

12. *In re* Application of United States for an Order (1) Authorizing the Use of a Pen Register & Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 384 F. Supp. 2d 562 (E.D.N.Y. 2005). Following a request for reconsideration by the government, Magistrate Judge James Orenstein acknowledged in an October 2005 opinion that he misinterpreted the SCA in his August 2005 opinion. *In re* Application of United States for an Order (1) Authorizing the Use of a Pen Register & Trap & Trace Device & (2) Authorizing Release of Subscriber &/or Cell Site Info., 396 F. Supp. 2d 294, 295, 302 n.4 (E.D.N.Y. 2005). Despite corrected reasoning in the later opinion, Magistrate Judge Orenstein still denied the government access to cell site location information on a showing of less than probable cause. *Id.* at 324.

13. For a list of cases addressing the issue, see the Table of Cases in Deborah S. Buckman, Annotation, *Allowable Use of Federal Pen Register & Trap & Trace Device to Trace Cell Phones & Internet Use*, 15 A.L.R. FED. 2D 537 (2006). There is also heated scholarship on the issue. *Compare* Bankston, *supra* note 7, at 589 (describing legal arguments made by the government for surveillance as "dubious at best and deceptive at worst"), *with* M. Wesley Clark, *Cell Phones as Tracking Devices*, 41 VAL. U. L. REV. 1413, 1413 (2007) (describing the advantages of wireless telephone tracking).

14. *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010).

15. Indeed, the magistrate judge whose decision was appealed noted: "Few Courts have . . . addressed in published opinion[s] whether the Government may nonetheless covertly obtain a cell phone subscriber's (or possessor's) *past*, or *historic*, movement/location information . . . . Some have suggested or credited . . . that it may; a few have concluded or suggested that it may not." *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 600 (W.D. Pa. 2008) (emphasis added). The appealed decision was also signed by the other magistrate judges in the district. *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 308. This likely provided additional incentive to the government to appeal, as it foreclosed the possibility that the government could submit rejected applications to magistrate judges more favorable to its position. *See infra* text accompanying note 183.

theory.[16] Thus, no appellate court has considered the viability of the government's super statute creation. The government seems unlikely to appeal a rejected application for *real time* cell site location information ostensibly authorized under the hybrid theory because of the risk of establishing unfavorable precedent. And, because of the ex parte and sealed nature of the applications, there is no defendant to appeal.

Even at the district court level, the government has responded to some judicial pushback by limiting its requests to location information derived from single cell towers, as opposed to more precise information derived from "triangulation" of multiple cell towers.[17] As Judge Lewis A. Kaplan of the Southern District of New York noted in his 2006 opinion, the government's self-imposed limitation is "apparently in the hope that applications for less detailed and invasive information w[ill] meet with a warmer judicial reception."[18] By carefully calculating its appeals and tailoring its requests for limited information, the government controls the status quo and limits the appellate courts' ability to reach the full issue. This seems to be often overlooked as an adverse implication of accepting the government's hybrid theory.

Part I of this Note provides an overview of cell site technology and describes the types of information sought, and often received, by the government when it submits applications requesting cell site location information. Part II explains current electronic surveillance law and provides a detailed analysis of the statutory basis of the government's asserted hybrid theory. Part III first describes the flaws of the theory, particularly in regard to the strained statutory interpretation required for its existence. It then suggests that wireless telephones used to obtain real time cell site location information are, for all practical purposes, tracking devices, which should require a showing of probable cause. Part IV discusses the adverse consequences of accepting the hybrid theory, including potential Fourth Amendment concerns and the lack of opportunity for appellate courts to reach the issue. The Note concludes by suggesting that the legislative and judicial branches of the federal government should take action to stop the proliferation of the hybrid theory.

I. WIRELESS TELEPHONE TECHNOLOGY

A. The Basics

The typical government application for cell site location information seeks court authorization for the installation and use of pen registers and trap-and-trace devices.[19] The location information sought is single or multiple cell site and

16. Instead, the government asserted authority under the SCA alone. *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 305. The court acknowledged district court decisions analyzing the hybrid theory in a footnote. *Id.* at 310 n.6.

17. For a detailed explanation of "triangulation," see *infra* note 53 and accompanying text.

18. *In re* Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 452 (S.D.N.Y. 2006).

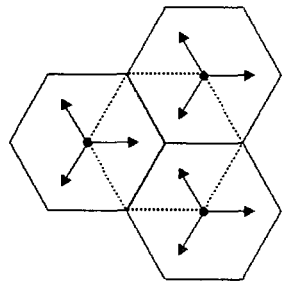
19. *See, e.g., id.* at 454.

sector/face data (physical address) .information at call origination (for outbound calls), call termination (for incoming calls), and, if reasonably available, during the progress of a call.[20] As is necessary to fully understand the government's requests for such information, this section provides a foundational overview of cell site technology and the information that can be obtained from pen registers and trap-and-trace devices.

To practically serve enormous geographic regions, wireless carriers divide the regions into numerous smaller areas, or cells.[21] Each cell can be conceptualized as three adjoining hexagons.[22] There is a base station tower (tower), with radio transmitters and receivers and one or more antennae, at the center of each hexagon.[23] Thus, for each cell, there are three towers. The "hexagonal union" of those three towers signifies a cell site.[24]

In Figure 1, the three solid hexagons, together, constitute a cell. The dots in the center of each of the hexagons represent the towers. The arrows protruding from the black dots represent the direction of the signals being transmitted from each tower. Finally, the dotted hexagon in the center represents the cell site, or the hexagonal union of the towers.

Figure 1[25]



The size of any given cell site is determined by multiple factors, including population density and topography.[26] Because of these factors, the radius of a cell can range "from many miles in suburban or rural areas to several hundred feet in

20. *See, e.g., id.*; *In re* Application of United States for an Order (1) Authorizing the Use of a Pen Register & Trap & Trace Device & (2) Authorizing Release of Subscriber &/or Cell Site Info., 396 F. Supp. 2d 294, 295, 296 (E.D.N.Y. 2005).

21. Declaration of Henry Hodor ¶ 10 (Feb. 23, 2006), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_4805_001_20091022.pdf. According to the information made publicly available in the Declaration, Mr. Hodor has served as a telecommunications consultant to the FBI since 1996. *Id.* ¶ 3. Mr. Hodor provided the Declaration with knowledge that the government would use it "in support of a request for authorization to use a pen register and trap and trace device." *Id.* ¶ 2.

22. *Id.* ¶ 10.

23. *Id.*; *see also In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 450.

24. Declaration of Henry Hodor, *supra* note 21, ¶ 12.

25. *Id.*

26. *Id.* ¶ 13.

urban areas."[27] Generally, cells are smaller in more densely populated wireless service areas.

To control multiple towers, wireless providers utilize a base station controller (base station).[28] Carriers also assign groups of cells within a wireless network to a mobile switching center.[29] Described as a "sophisticated computer," the mobile switching center manages the communication between wireless telephones and all base stations in a wireless service area.[30] In order for a wireless network to be able to carry calls on tens of thousands and sometimes hundreds of thousands of wireless telephones, the network maintains "approximate fixes" on the telephones.[31] Thus, anytime a wireless telephone is turned on "it periodically transmits a unique identification number [through both the base station and mobile switching center] to register its presence and location in the network."[32]

To make or receive calls, a wireless telephone must be within signal range of a tower.[33] A tower transmits and receives signals in a 360-degree range.[34] That range is typically divided into three equal 120-degree sectors.[35] Sensors in the base station detect which tower and which sector make signal contact with the wireless telephone, thus providing an indication—within a 120-degree arc from the tower—of the direction in which the wireless telephone lies.[36]

As a wireless telephone moves, the tower receiving the strongest signal may change, as often occurs when a wireless telephone is transported to a position closer to a different tower.[37] When this happens, the mobile switching center controls the handover between towers associated with different base stations to ensure the continuity of the call in progress.[38]

It should be noted that a wireless telephone does not always make contact with the tower that is physically the closest.[39] Large buildings or other interference can hinder transmission, resulting in a wireless telephone receiving better signal

---

27. *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 450.

28. Declaration of Henry Hodor, *supra* note 21, ¶ 10.

29. *Id.* ¶ 14.

30. *Id.*

31. *Id.* ¶ 18.

32. *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 450. The network registration process takes place even when telephone calls are not being made or received. *Id.*

33. *Id.*

34. Declaration of Henry Hodor, *supra* note 21, ¶ 11.

35. *Id.*

36. *Id.*

37. *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 450.

38. Declaration of Henry Hodor, *supra* note 21, ¶ 14. "Failures in this handling function doubtless account for a great many of the 'dropped calls' that so aggravate cellular telephone users." *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 450 n.2.

39. Declaration of Henry Hodor, *supra* note 21, ¶ 11.

strength from a tower that is not the closest in proximity.[40] However, the location of the tower receiving a signal from a wireless telephone "at any given moment inherently fixes the general location of the phone."[41]

B. Recording and Disclosure of Cell Site Location Information

The Communications Assistance for Law Enforcement Act (CALEA),[42] which became effective in 1998, requires, among other things, that the equipment and service of telecommunications carriers be capable of "expeditiously isolating and enabling the government, pursuant to court order or other lawful authorization, to intercept call-identifying information."[43] To ensure wireless carriers' compliance with CALEA, the industry developed a technical standard that is known as the "J-Standard."[44]

The J-Standard delineates "the services and features carriers must provide to support electronic surveillance and the interfaces necessary to deliver intercepted information to law enforcement."[45] The intercepted information is theoretically available in real time, as the J-Standard requires carriers to transmit it within eight seconds.[46]

After obtaining a court order authorizing the disclosure of cell site location information, the government receives a report of all the calls made and received by a specific wireless telephone, the date of the calls, and the start and end time of the calls.[47] Most relevant here, the government also receives a listing of the numbers assigned to the tower, and a number indicating the 120-degree sector or triangular area of the face of that tower, with which the telephone is communicating during its calls.[48] The tower numbers correspond to exact physical locations of the towers.[49]

Wireless carriers use this information for various purposes, such as determining roaming charges and tracking call volume by location.[50] When the

---

40. *Id.*

41. *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 451.

42. 47 U.S.C. §§ 1001–1010 (2006).

43. § 1002(a)(2).

44. *In re* Application of United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, (2) Access to Customer Records, & (3) Cell Phone Tracking, 441 F. Supp. 2d 816, 820 (S.D. Tex. 2006); *see also* David L. Sobel, *Privacy and Law Enforcement in the Digital Age*, COMM. LAW., Winter 2001, at 3, 5. The industry's technical specification for the J-Standard is ANSI/J-STD-025A. Declaration of Henry Hodor, *supra* note 21, ¶ 6.

45. Sobel, *supra* note 44, at 5.

46. Declaration of Henry Hodor, *supra* note 21, ¶ 29.

47. *In re* Application of United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 437 (S.D.N.Y. 2005).

48. *Id.*

49. *See id.*

50. *In re* Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 451 (S.D.N.Y. 2006).

government uses the information, however, it is typically to determine, at minimum, the exact physical location of the tower with which a wireless telephone is communicating and the 120-degree arc off the face of that tower.[51] This information enables law enforcement officers to track an individual's general geographic movement.[52]

Moreover, the government can use a wireless telephone's communication with two or more towers to ascertain precise location information. Judge Kaplan provided a clear account of the triangulation process in his 2006 opinion:

> Triangulation is the process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points. While only the length of one side of the triangle is known at first (the side connecting the two known points), simple trigonometry reveals the lengths of the other sides and so the position of the third point. In the context of cell site information, the two known points are the antenna towers, the third point is the cellular telephone, and the direction from each tower to the phone is discerned from the information about which face of each tower is facing the phone.[53]

Wireless telephones also now have global positioning system (GPS) technology capabilities, which can provide precise location information. While the government is likely to assert authority to obtain location information derived from GPS technology,[54] analysis of those requests is beyond the scope of this Note. Even without GPS technology, however, the government can derive expansive tracking capabilities from cell site data. The government thus sees such information as "an important investigatory tool," which can be instrumental to

---

51. *See In re* Application of United States for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (discussing "Wireless Location Technology" and "Data Collection and Retention").

52. *Id.*

53. *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 451 n.3. In the same footnote, Judge Kaplan described another tracking process, also known as triangulation:

> Another method of tracking the location of cellular telephones, which also is sometimes called triangulation, is possible when a phone transmits signals to three antenna towers at once. Based on the strength of a phone's signal to a tower, and the time delay for the signal to reach the tower, one can determine the distance between the phone and the tower. One can then draw around the tower a circle, the radius of which is the distance from that tower to the phone. The location of the phone can be pinpointed by drawing circles around three [or] more towers and seeing where the circles intersect.

Id.

54. *See, e.g., In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 311 (3d Cir. 2010) ("[T]he Government does not argue that it cannot or will not request information from a GPS device through a § 2703(d) [of the SCA] order.").

"help[ing] determine where to establish physical surveill[a]nce and . . . help[ing] locate kidnapping victims, fugitives, and targets of criminal investigations."[55] The asserted hybrid theory is the government's creative attempt to obtain the information without having to meet the typically applicable probable cause standard.

II. THE HYBRID THEORY

The hybrid theory is based on an assertion that the Pen/Trap Statute[56] and the SCA[57] can be combined so that the statutes, together, authorize the government to obtain *prospective* cell site location information without a showing of probable cause.[58] The authority does not exist under either statute alone,[59] but the federal government asserts it is created when the two statutes are combined.[60] The Pen/Trap Statute and the SCA are part of the Electronic Communications Privacy Act (ECPA) of 1986.[61] The ECPA is the statutory authority for electronic surveillance law.[62]

The ECPA divides electronic surveillance into four broad categories: (1) wiretaps;[63] (2) tracking devices;[64] (3) stored communications and subscriber

---

55. *In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d at 451–52 (citing the government's brief).

56. 18 U.S.C. §§ 3121–3127 (2006 & Supp. 2009).

57. 18 U.S.C. §§ 2701–2712 (2006).

58. *See, e.g.*, *In re* Application of United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed], 416 F. Supp. 2d 390, 391 (D. Md. 2006) ("[T]he government . . . outlin[ed] its position that an order to obtain prospective cell site information can be entered upon less than probable cause pursuant to the combined authority of 18 U.S.C. § 3121 *et seq.* (the 'Pen/Trap Statute') and 18 U.S.C. § 2701 *et seq.* (the 'SCA').").

59. CALEA explicitly prohibits service providers from releasing "any information that may disclose the physical location of the subscriber" if the government is acting "solely pursuant to the authority for pen registers and trap and trace devices." 47 U.S.C. § 1002(a)(2)(B) (2006). Similarly, the information available under the SCA is limited to *historical* (as opposed to prospective) data. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) (discussing the lack of procedural features in the SCA that are associated with prospective surveillance). For more discussion of these limitations, see *infra* Part III.A.

60. *See, e.g.*, *In re Application of United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed]*, 416 F. Supp. 2d at 391.

61. Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.).

62. *See, e.g.*, *In re* Application of United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294, 304 (E.D.N.Y. 2005) ("Despite frequent amendment, the basic architecture of electronic surveillance law erected by the ECPA remains in place to this day.").

63. 18 U.S.C. §§ 2510–2522 (2006).

64. 18 U.S.C. § 3117 (2006).

records (SCA);[65] and (4) pen registers and trap-and-trace devices (Pen/Trap Statute).[66] The ECPA provides different legal standards for each category: wiretaps require a "super-warrant";[67] tracking devices require probable cause under Rule 41 of the Federal Rules of Criminal Procedure;[68] the SCA requires specific and articulable facts that the information will be relevant to an ongoing criminal investigation;[69] and the Pen/Trap Statute requires showing that the information will be relevant to an ongoing criminal investigation.[70] To obtain court approval for surveillance under one of the four categories, the government must meet the burden required by the respective category. The burdens increase as the forms of surveillance become more intrusive.[71]

The hybrid theory starts with an interpretation of the Pen/Trap Statute. The statute regulates the government's use of pen registers and trap-and-trace devices.[72] Traditionally, a pen register recorded the numbers dialed for outgoing calls made from a telephone, and a trap-and-trace device captured the incoming numbers of calls made to a telephone.[73] To obtain court approval to use pen registers and trap-and-trace devices, the government needed to show that the information likely to be obtained was relevant to an ongoing criminal investigation.[74] This burden, the lowest required for electronic surveillance under the ECPA, was justified by the minimal intrusiveness of the technology.[75]

In 2001, the USA PATRIOT Act (PATRIOT Act)[76] expanded the

---

65. 18 U.S.C. §§ 2701–2712 (2006).

66. 18 U.S.C. §§ 3121–3127 (2006 & Supp. 2009).

67. 18 U.S.C. § 2518. The term "super-warrant" is used because, to install a wiretap, the government must show probable cause—the standard for more traditional warrants—*and* establish that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *In re Application of United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info.*, 396 F. Supp. 2d at 305 (quoting 18 U.S.C. §2518(3)(c)).

68. *See* 18 U.S.C. § 3117; *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005) ("The ECPA was not intended to affect the legal standard for the issuance of orders authorizing these devices. A Rule 41 probable cause warrant was (and is) the standard procedure for authorizing the installation and use of mobile tracking devices." (citations omitted)).

69. 18 U.S.C. § 2703(d).

70. 18 U.S.C. § 3123(a).

71. *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 753.

72. *See* 18 U.S.C. § 3121.

73. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 749.

74. 18 U.S.C. § 3123(a).

75. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (rejecting petitioner's argument that he had a "legitimate expectation of privacy" in the telephone numbers he dialed); *see also In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 752–53 (stating that because of the holding in *Smith*, the "legal hurdle" for the authorization to use pen registers and trap-and-trace devices is very low).

76. Uniting and Strengthening America by Providing Appropriate Tools

definitions of pen registers and trap-and-trace devices. Section 3127 of the Pen/Trap Statute now defines a pen register as "a device or process which records or decodes dialing, routing, addressing, or *signaling information* transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[77] A trap-and-trace device is defined as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and *signaling information* reasonably likely to identify the source of a wire or electronic communication."[78] These expanded definitions, particularly the addition of the term "signaling information," increase the scope of information available to the government under the Pen/Trap Statute.[79] Despite the availability of additional information, the legal burden on the government to obtain that information remains the same.[80]

As explained more fully below, the hybrid theory rests, in part, on the assumption that cell site location data is "signaling information" under the expanded Pen/Trap Statute definitions.[81] Despite cell site location information falling within the expanded definitions, the data cannot be obtained under the authority of the Pen/Trap Statute alone. CALEA prohibits service providers from releasing "any information that may disclose the physical location of the subscriber," if the government is acting "*solely* pursuant to the authority for pen registers and trap and trace devices."[82] Cell site data, by its nature, "may disclose the physical location of the subscriber."[83] Thus, the government may not obtain cell site location information under the Pen/Trap Statute without some other authority.

The hybrid theory asserts that the additional authority needed is found in the SCA.[84] The SCA, like the Pen/Trap Statute, is part of the ECPA. The SCA

Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

77. 18 U.S.C. § 3127(3) (emphasis added).

78. 18 U.S.C. § 3127(4) (emphasis added).

79. For a discussion of this point, see Steven B. Toeniskoetter, *Preventing a Modern Panopticon: Law Enforcement Acquisition of Real-Time Cellular Tracking Data*, 13 RICH. J.L. & TECH. 16, 64–67 (2007).

80. The legal burden is codified at 18 U.S.C. § 3123(a), which was not amended by the PATRIOT Act.

81. *See, e.g.*, *In re* Application of United States for an Order Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211, 214 (W.D.N.Y. 2006) ("[C]ell site location data is encompassed by the term 'signaling information' when the term was added to the Pen Statute by Congress in 2001 as part of the Patriot Act[.]").

82. 47 U.S.C. § 1002(a)(2)(B) (2006) (emphasis added).

83. For an explanation of what constitutes cell site location data, see *supra* Part I.B.

84. *See, e.g.*, *In re* Application of United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed], 416 F. Supp. 2d 390, 393 (D. Md. 2006) ("The necessary authority for the disclosure of cell-site information called for by the Pen/Trap Statute is provided by Section 2703 of the SCA." (quoting the government's brief)).

governs the disclosure of "record[s] or other information pertaining to a subscriber to or customer of [an electronic communication service]."[85] In order to obtain such historical data under the SCA, the government must provide specific and articulable facts that demonstrate the information will be relevant to an ongoing criminal investigation.[86] On the continuum of legal standards required for electronic surveillance under the ECPA, this standard is higher than required by the Pen/Trap Statute but lower than probable cause.[87]

The hybrid theory asserts that cell site location information falls within the authority of the SCA because it is "information pertaining to a subscriber."[88] Like the Pen/Trap Statute, however, the SCA alone does not give the government the information it seeks. The SCA permits the disclosure of *historical*, not *real time*, data.[89]

To overcome the SCA's historical-data limitation, the hybrid theory circles back to the Pen/Trap Statute.[90] Specifically, the theory asserts that disclosure of cell site location information is authorized by the SCA and can be collected in *real time* by virtue of the Pen/Trap Statute.[91] Thus, the location information falls within the SCA category of the ECPA and is obtainable upon establishing specific and articulable facts that the information will be relevant to an ongoing criminal investigation.[92]

The hybrid theory essentially allows the government to circumvent the statutory limitations of both the Pen/Trap Statute, as outlined in CALEA, and the SCA. The prohibition in CALEA that location information cannot be obtained under the authority of the Pen/Trap Statute is overcome by the SCA, and the limitation in the SCA that information cannot be obtained in real time is overcome by the Pen/Trap Statute. This circular argument creates more expansive authority under a hybrid of two statutes than exists under either statute alone. If accepted, the hybrid theory gives the government access to *real time* cell site location information upon meeting the "specific and articulable facts" standard that governs the SCA.[93]

---

85. 18 U.S.C. § 2703(c)(1) (2006).

86. 18 U.S.C. § 2703(d).

87. *See supra* text accompanying notes 68–70.

88. *See, e.g.*, *In re Application of United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] & [Sealed]*, 416 F. Supp. 2d at 393 (quoting the government's brief).

89. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005).

90. *Id.* at 761.

91. *Id.*

92. *Id.*

93. 18 U.S.C. § 2703(d) (2006).

III. FLAWS OF THE HYBRID THEORY

A. There Is No Indication the Pen/Trap Statute and the SCA Should be Combined to Create More Expansive Authority Than Under Either Statute Alone

Proponents of the hybrid theory contend that the limiting language in CALEA—which states "information acquired *solely pursuant* to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber"[94]—permits government agencies to combine the Pen/Trap Statute with the SCA in order to obtain real time cell site location information.[95] The reasoning seems to be that the word "solely" indicates access to information *precluded* by § 1002(a)(2)(B) may be *included* if the Pen/Trap Statute is partnered with the SCA.

The largest obstacle to the hybrid theory is that the SCA does not indicate that it should be read in conjunction with, and thus expand the scope of, the Pen/Trap Statute.[96] Indeed, with one exception, the statutes do not cross-reference one another: the Pen/Trap Statute does not mention the SCA or CALEA; § 2703 of the SCA does not mention CALEA or the Pen/Trap Statute; and the "solely pursuant" provision of CALEA does not mention the SCA.[97] While CALEA does mention the Pen/Trap Statute, it is "only in the negative sense of disclaiming its applicability."[98] That is, CALEA refers to "the authority for pen registers and trap and trace devices"—the Pen/Trap Statute—only to assert that information obtained under that authority may not disclose the physical location of a wireless telephone subscriber.[99] This cross-reference contradicts a suggestion that Congress intended CALEA and the Pen/Trap Statute be combined. Moreover, if Congress intended any of the other relevant statutory provisions be combined to provide the government with more authority than any of the statutes alone provide, one would expect to read that congressional intent in the plain language of the statutes.[100] Instead, the plain language points to a lack of such intent.

The chronology of the legislation also gives little indication that Congress intended the statutes be combined.[101] Congress enacted the relevant statutes at various times over a fifteen year period (1986–2001). Congress enacted the Pen/Trap Statute as part of the ECPA in 1986.[102] CALEA, with its critically

---

94. 47 U.S.C. § 1002(a)(2)(B) (2006) (emphasis added).

95. *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 761.

96. Magistrate Judge Stephen Wm. Smith of the Southern District of Texas first presented this problem in his 2005 opinion. *Id.* at 764.

97. *Id.*

98. *Id.*

99. *See* 47 U.S.C. § 1002(a)(2)(B).

100. *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 764.

101. Again, Magistrate Judge Smith of the Southern District of Texas first presented this issue in 2005. *See id.* at 765.

102. Electronic Communications Privacy Act of 1986, Pub. L. 99-508, tit. III, § 301(a), 100 Stat. 1868.

important "solely pursuant" phrase, was passed in 1994 and became effective in 1998.[103] Congress did not pass the PATRIOT Act, which purportedly expanded the scope of the Pen/Trap Statute to cover the cell site data sought by the government, until 2001.[104] Prior to 2001, without the expanded Pen/Trap Statute definitions, the government had no basis to the claim that the Pen/Trap Statute covered cell site data—the earlier definitions only covered numbers dialed or received, not "signaling information."[105] The resulting inference that in 1994 Congress intended the phrase "solely pursuant" in CALEA to mean the government could obtain otherwise prohibited location information under the Pen/Trap Statute based on definitions Congress would not expand for another seven years simply reaches too far.[106]

Furthermore, the respective limitations of the Pen/Trap Statute and the SCA suggest that Congress did not intend their combination.[107] Under the Pen/Trap Statute, the original definitions of pen registers and trap-and-trace devices allowed for disclosure of only telephone numbers.[108] The disclosure of physical location when the devices were used on land-line telephones was an incidental result of the technology at that time. In addition to being incidental, the location information was static and could not be used to track an individual's movement. Now, through CALEA, Congress has explicitly stated that location information is not available under the Pen/Trap Statute.[109] Congress has also indicated that real time information is not available under the SCA.[110] It thus seems illogical to conclude that Congress intended one word, "solely," to overcome the location limitation of the Pen/Trap Statute and the historical limitation of the SCA to provide the government with more disclosure than it has under either statute alone.[111]

Finally, there is no other statutory context in which the hybrid theory has been used.[112] As one scholar explained, "The government, in support of its hybrid theory, has never cited another similar arrangement, where two independent statutes are combined to obtain a result that neither authorizes separately."[113] The hybrid theory creates a super statute from the combination of the Pen/Trap Statute

---

103. Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2006).

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

105. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 765.

106. For a similar explanation of this argument, see *id.*

107. For a more detailed discussion of the statutes' limitations, see *supra* Part II.

108. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 749.

109. 47 U.S.C. § 1002(a)(2)(B) (2006).

110. *See* Bankston, *supra* note 7, at 608 & nn.83–86 (discussing the lack of procedural features in the SCA that are associated with prospective surveillance).

111. As Steven B. Toeniskoetter noted in his 2007 article, "One commentator has attacked this theory on the grounds that '0 + 0 = 0.'" Toeniskoetter, *supra* note 79, at 80.

112. *See id.*

113. *Id.*

and the SCA and provides the government with more information than it is entitled to under either statue alone. By overcoming the limitations of Pen/Trap Statute and the SCA, the government relies on authority that was never approved by the legislature.

B. Wireless Telephones Used to Obtain Real Time Cell Site Location Information Act as Tracking Devices and Thus Should be Subject to the Probable Cause Standard

To obtain surveillance information that falls within the SCA category of the ECPA, the government must only show specific and articulable facts that the information is relevant and material to an ongoing criminal investigation.[114] Under this standard, the government may only require "provider[s] of electronic communication service[s]" to disclose information.[115] The SCA defines an electronic communication service as "any service which provides to users thereof the ability to send or receive *wire or electronic communications*."[116] Thus, if cell site location information is either a wire or electronic communication, authority for its disclosure may fall under the SCA.

The SCA defines both "wire communications" and "electronic communications." Significantly, the definition of electronic communications expressly excludes "any communication from a tracking device," as it is defined in § 3117 of the ECPA.[117] Under § 3117, a "tracking device" is "an electronic or mechanical device which permits the tracking of the movement of a person or object."[118] This definition contains very few qualifiers. It does not require that a device be designed or intended as a tracking device or that a device have no function other than tracking.[119] Furthermore, the definition makes no qualification as to how precise a device's tracking capability must be.[120]

The disclosure of cell site location information enables the government to, at minimum, place a wireless telephone within a 120-degree triangular area off the face of a cell tower (the exact physical location of which is known to the government) and also to track that telephone's movement from one cell tower to another.[121] Even more precise location information is available to the government through triangulation, and the technology exists to disclose the information in real time.[122] In this way, a wireless telephone "permits the tracking of the movement of a person or object" and falls within ECPA's definition of a tracking device.[123] It

---

114. 18 U.S.C. § 2703(d) (2006).

115. § 2703(c)(1).

116. 18 U.S.C. § 2510(15) (2006) (emphasis added) (incorporated into the SCA by 18 U.S.C. § 2711(1) (2006)).

117. § 2510(12)(C) (incorporated into the SCA by § 2711(1)).

118. 18 U.S.C. § 3117(b) (2006).

119. *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 753 (S.D. Tex. 2005).

120. *Id.*

121. *See* discussion *supra* Part I.B.

122. *See* discussion *supra* Part I.B.

123. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 757 (concluding that "prospective cell site data is

follows that because cell site location information is "information from a tracking device"—in this case, a wireless telephone—the information is unobtainable under the SCA's specific and articulable facts standard. The government should, instead, be required to meet probable cause under Rule 41 of the Federal Rules of Criminal Procedure.[124]

In a recent opinion, the Third Circuit avoided the conclusion that cell site location information is information from a tracking device by finding that *historical* cell site location information "is derived from a 'wire communication.'"[125] Unlike electronic communication, the SCA definition of a wire communication does not expressly exclude information from a tracking device.[126] Thus, the Third Circuit reasoned that "even if the record of a cell phone call does indicate generally where a cell phone was used when a call was made, so that the resulting [cell site location information] was information from a tracking device, that is irrelevant here."[127] The problem with this conclusion is that the SCA's definition of wire communication seems to contemplate only communication involving the human voice.[128] Cell site location information does not fall within this definition, and thus cannot fall outside the SCA's tracking device exclusion by being classified as wire communication.[129]

Although some courts, including the Third Circuit, have suggested that cell site location information is not "tracking" information because it only provides the government with a general geographic location of a suspect,[130] there is no such statutory distinction between this and more exact location information. Under § 3117, as long as a device "permits the tracking of the movement of a person or thing," it is considered a tracking device irrespective of how precisely an

---

properly categorized as tracking device information under § 3117").

124. 18 U.S.C. § 3117 (2006); *see also id.*

125. *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 310 (3d Cir. 2010).

126. *See* 18 U.S.C. § 2510(1) (2006) (incorporated into the SCA by 18 U.S.C. § 2711(1) (2006)).

127. *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 310.

128. *See* 18 U.S.C. §§ 2510(1), (18) (2006) (incorporated into the SCA by § 2711(1)) (defining "wire communication" as any "any aural transfer made in whole or in part through the use of facilities for the transmissions of communications by the aid of wire, cable, or other like connection" and "aural transfer" as "a transfer containing the human voice at any point between and including the point of origin and point of reception); *see also In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 759.

129. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 759 (citing *United States v. Forest*, 355 F.3d 942, 949 (6th Cir. 2004)).

130. *See, e.g., In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 311; *In re* Application of United States for an Order for Disclosure of Telecomms. Records & Authorizing the Use of a Pen Register & Trap & Trace, 405 F. Supp. 2d 435, 440 (S.D.N.Y. 2005) (qualifying cell site data as disclosing physical location "only in the roughest manner").

investigator can follow it. Moreover, as will be discussed below, if the hybrid theory is accepted, there is nothing to restrict the government from obtaining precise cell site location information.[131] And, when real time cell site location information is used to locate individuals inside their homes, the disclosure of that information implicates constitutional concerns under the Fourth Amendment.[132]

IV. IMPLICATIONS OF ACCEPTING THE HYBRID THEORY

A. The Hybrid Theory Implicates Fourth Amendment Concerns Because It Does Not Impose Necessary Limits on Information Available to the Government Where There Is Less Than Probable Cause

The government can set an artificial boundary by asking for only limited cell site location information, thereby tailoring its request to current judicial response.[133] In the past, the government submitted applications seeking court authorization to obtain unlimited real time cell site location information.[134] On at least one occasion, the United States admitted that its request for limited location information was purely in response to judicial opposition to its previous requests for unlimited location information.[135] Under the statutes, there is no distinction between obtaining location information from one cell tower instead of from multiple cell towers, nor from obtaining location information only when a telephone is in use, instead of any time it is in the "on" position.[136]

---

131. *See* discussion *infra* Part IV.A.

132. *See* discussion *infra* Part IV.A.

133. *See, e.g.*, *In re* Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., No. 06 Crim. Misc. 01, 2006 WL 468300, at *2 (S.D.N.Y. Feb. 28, 2006) ("[W]hile the Government's request for cell site location information in this District has been limited to general tower location . . . and only for the origination and termination of calls, the Government's statutory interpretation would allow it to obtain triangulation location information for the entire duration of the call and, indeed, for all times the cell phone is on, even when no call is in progress.").

134. *See, e.g.*, *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d at 748–49.

135. *In re* Application of United States for Orders Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. Under 18 U.S.C. § 2703, 415 F. Supp. 2d 211, 218 (W.D.N.Y. 2006); *see also In re Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 2006 WL 468300, at *2. Similarly, in its recent appeal to the Third Circuit, the government limited its request to *historical* cell site location information, but "d[id] not foreclose the possibility that in a future case it w[ould] argue that the SCA may be read to authorize disclosure of additional information." *In re Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 308.

136. The hybrid theory assumes cell site location information qualifies as "signaling information" under provision 18 U.S.C. § 3127(3) of the Pen/Trap Statute and as "information pertaining to a subscriber" under § 2703(c)(1) of the SCA. Within these definitions, there is no distinction regarding the specificity of the information. *See In re Application of United States for Orders Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111 & the Disclosure of Subscriber & Activity Info. under 18 U.S.C. § 2703*, 415 F. Supp. 2d at 219; *see also In re*

The artificial constraint to single cell site location information, therefore, acts as a self-imposed check on the government. If the hybrid theory is accepted, there is nothing to stop the government from reverting back to its initial requests for unlimited cell site location information. The government could retrieve the information upon meeting a standard less than probable cause, allowing law enforcement officers to track the movement of suspects and discern those individuals' locations inside their homes without obtaining a warrant. Such a result is a troubling departure from established constitutional standards.

Indeed, in *United States v. Karo* the Supreme Court held that monitoring a tracking beeper in a private residence violated the Fourth Amendment rights of those who had a privacy interest inside the home.[137] The Court reiterated previous holdings that individuals have an expectation of privacy within their residences and that society is willing to recognize that expectation as reasonable.[138] The Court stated:

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article—or a person, for that matter—is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.[139]

Two years earlier, in 1979, the Supreme Court held that state police did not violate a petitioner's Fourth Amendment rights when agents installed a pen register on the petitioner's home telephone without first obtaining a warrant.[140] But in 1979 the information available from pen registers was profoundly different than it is today. In *Smith*, the government used a pen register only to obtain a list of telephone numbers dialed from the petitioner's home telephone.[141] The government now asserts the authority to use pen registers to track the movement of individuals, both inside and outside of their homes.[142] As the Supreme Court stated in *Karo*, "It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."[143]

Application of United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 2006 WL 468300, at *2.

137. 468 U.S. 705, 714 (1984).

138. *Id.* at 714–15 (citing Welsh v. Wisconsin, 466 U.S. 740, 748–49 (1984); Steagald v. United States, 451 U.S. 204, 211–12 (1981); Payton v. New York, 445 U.S. 573, 586 (1980)).

139. *Id.* at 716.

140. Smith v. Maryland, 442 U.S. 735, 741–42 (1979).

141. *Id.* at 735.

142. *See* Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 444 (2007) ("Cell phone location tracking—at least with presently-existing technology—cannot help but implicate the home.").

143. *Karo*, 468 U.S. at 712.

In *Smith*, the government did not exploit pen register technology because the petitioner held no reasonable expectation of privacy in the information collected.[144] Conversely, individuals do hold reasonable expectations of privacy inside their homes.[145] When the government asserts the right to use pen registers to track the movement of individuals and to ascertain those individuals' location inside their private residences, the government exploits pen register technology in a way that, under *Karo*, deserves Fourth Amendment scrutiny.

Furthermore, the holding in *Karo* is not limited only to tracking beepers.[146] Wireless telephones are presumably "electronic device[s]" that, because of their mobile nature, regularly move in and out of private areas, such as homes. When government agents use information derived from wireless telephones to track the movement of individuals, the agents can tell whether those individuals are in their homes at particular times. Such use of wireless telephones is again precisely the type of intrusion that, under the Court's holding in *Karo*, raises Fourth Amendment concerns.[147]

In some applications, the government limits its requests to only historical—as opposed to real time—cell site location information.[148] This limit is more statutorily legitimate, as historical information is likely available to the government under the authority of the SCA alone.[149] In its recent opinion, the Third Circuit refused to conclude that cell site location information "by definition should be considered information from a tracking device" and thus subject to probable cause.[150] The court left open the possibility, however, that there may be privacy implications if the information is used to obtain present location information: "If it can be used to allow the inference of present, or even future, location, in this respect [cell site location information] may resemble a tracking device which provides information as to the actual whereabouts of the subject."[151] This distinction between historical and real time cell site location information is important, as the legal standard for government access to cell site location information should depend on the type of information sought.[152]

---

144. *Smith*, 442 U.S. at 741–42.

145. *Karo*, 468 U.S. at 714.

146. *Id.* at 716.

147. *See* McLaughlin, *supra* note 142, at 438. In his analysis, McLaughlin noted that because wireless telephones constantly move in and out of houses, it would be difficult to track wireless telephones only outside the house. Because the government cannot intrude into houses without warrants, it is hard to support any conclusion other than requiring the government to obtain a warrant to engage in wireless telephone tracking. *Id.*

148. *See, e.g.*, *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 305 (3d Cir. 2010)

149. *Id.* at 313 (holding that historical cell site location information may be available to the government upon meeting the SCA's specific and articulable facts standard).

150. *Id.* at 313.

151. *Id.* at 312.

152. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005) ("The legal threshold for each type of communication is different, notwithstanding that a cell phone transmits them all.").

When the government obtains real time cell site location information, wireless telephones are, for all practical purposes, being used as tracking devices.[153] Thus, the government should be required to show probable cause to acquire the information.[154] If wireless telephones, regardless of the information the government may obtain from those telephones, fall outside the statutory definition of "tracking device," this creates a loophole that effectively eliminates the probable cause requirement: "[L]aw enforcement could simply install cell phones in place of the [tracking] beepers currently under vehicles and inside drum barrels, and eliminate forever the need to obtain a Rule 41 search warrant for tracking surveillance."[155] Such a result would not comport with the established constitutional standards discussed above.

B. The Only Party with an Incentive to Appeal Orders Authorizing the Government to Obtain Real Time Cell Site Location Information Without a Showing of Probable Cause Rarely has Knowledge that the Surveillance Took Place

Applications for the use of pen registers and trap-and-trace devices are routinely submitted ex parte and under seal. The government is understandably not required to notify individuals that their movements are being tracked during the course of a criminal investigation,[156] but the justification for not providing notice is lost at the conclusion of criminal proceedings. It is disturbing that no after-the-fact notice is ever given to the vast majority of monitored individuals to inform them that the government obtained their location information.[157] Because applications and orders are routinely required to remain sealed "until otherwise ordered by the court,"[158] unsealing necessitates what United States Magistrate Judge Stephen Wm. Smith once termed "judicial vigilance."[159] Without it, "temporary sealing all too easily becomes permanent sealing."[160]

Although the available statistics are admittedly limited, the judiciary's "vigilance" seems to be seriously lacking. The anecdotes are startling. From the period of 1995 until 2007, Houston magistrate judges issued 3886 sealed electronic surveillance orders.[161] As of 2009, 3877, or 99.8%, of the orders remained under seal, even though the criminal investigations had long been closed.[162] When one considers the number of orders that remain under seal in the larger national context, it reveals the secrecy involved in electronic surveillance. The nearly 4000 electronic surveillance orders that remain sealed indefinitely in Houston represent the work of only one percent of the approximately 560 magistrate judges currently

153. *Id.* at 757.
154. *Id.*
155. *Id.* at 756.
156. Smith, *supra* note 10, at 209.
157. *Id.*
158. *Id.*
159. *Id.* at 209–10.
160. *Id.* at 210.
161. *Id.* at 209.
162. *Id.*

seated in U.S. federal courts.[163]

Notably, the Supreme Court does not seal its opinions.[164] The Court last addressed the issue of public access to judicial opinions in 1888,[165] at which time the concept of public access was firmly rooted and accepted.[166] Indeed, the concept dates back at least to eleventh-century England.[167] By the sixteenth century, and in succeeding centuries, the defining characteristic that distinguished England's common law from Continental Europe's civil law was free access to the courts.[168] This "revered" policy followed the colonists to America.[169] It was not until the end of the twentieth century that the United States began to see significant exceptions to the general rule of access to the courts.[170] These exceptions, however, drew a distinction between judicial rulings[171] and case-related filings:[172] "[A]t common law, and for most of this nation's history, judgments and decrees were not withheld from public view."[173]

Given this history and the Supreme Court's precedent, it is difficult to justify the notion that individuals whose movements have been tracked via their wireless telephones are rarely given notice that such surveillance ever took place, even long after any pending criminal proceedings have concluded.[174] As Magistrate Judge Smith acknowledged, "If the Supreme Court has found no occasion to conduct its business in secret or even to assert such a power in theory, it is difficult to understand why lower courts should do so."[175]

In addition to the apparent lack of "vigilance" among lower court judges, existing statutory law further compounds the secrecy problem. The Pen/Trap Statute and the SCA contain no or limited notice requirements.[176] The Pen/Trap Statute does not require any notification that the surveillance is going to, or ever did, take place.[177] Similarly, the SCA only requires prior notice when the

---

163. *Id.* at 211.

164. *See* Hicklin Eng'g, L.C. v. Bartell, 439 F.3d 346, 348–49 (7th Cir. 2006) ("The Supreme Court issues public opinions, even those said to involve state secrets.").

165. *See* Banks v. Manchester, 148 U.S. 244 (1888).

166. Smith, *supra* note 10, at 193–94.

167. *Id.* at 182.

168. *See id.* As one foreign observer described: "The publicity of [England's] proceedings is indeed astonishing. Free access to the courts is universally granted." *Id.* at 183 (quoting CHRISTIAN AUGUST GOTTLIEB GÖDE, A FOREIGNER'S OPINION OF ENGLAND, ENGLISHMEN, ENGLISHWOMEN, ENGLISH MANNERS, ENGLISH MORALS 214 (Thomas Horne trans., 1822)).

169. *Id.* at 190.

170. *Id.* at 201–02.

171. In his article, Magistrate Judge Smith described "judicial rulings" as "documents authored or generated by the court itself in discharging its judicial function, including opinions, orders, judgments, and docket sheets." *Id.* at 206.

172. *Id.*

173. *Id.*

174. *Id.* at 209.

175. *Id.* at 207.

176. *See* Bankston, *supra* note 7, at 632–33.

177. *See id.* at 632.

government uses certain judicial proceedings to obtain the orders,[178] and even those requirements can be easily overcome.[179] The government can delay the notice requirement "merely by certifying that prior notice . . . would harm [the government's] investigation."[180] Lastly, the government, not the court, is responsible for providing the notice.[181] Section 2703(b) of the SCA states that notice comes "from the governmental entity" seeking the information.[182] There is no incentive for the government to provide notice and no oversight for whether the notice is actually being given.

Furthermore, the government has little to no incentive to appeal rejected orders, because it does not want to risk the court setting unfavorable precedent. Magistrate Judge Smith explained that if the government's application gets denied, the government can simply wait until a different magistrate judge is on duty and then submit its application again.[183] Indeed, despite pleas by lower courts for appellate guidance,[184] the government has only appealed one decision to a Circuit Court of Appeals. And the government's choice to appeal that particular decision to the Third Circuit was undoubtedly calculated, as the magistrate judge went beyond most other courts in limiting the government's access to information.[185]

The Third Circuit opinion, moreover, provides little guidance to magistrates. The court held that the government may be entitled to historical cell site location information upon meeting the specific and articulable facts standard under the SCA.[186] However, the court later stated that magistrates are not required to release the information upon the lesser showing.[187] That is, magistrates have discretion to require the government to meet a higher standard, such as probable cause. Furthermore, because the government in that appeal asserted authority under the SCA alone, there was no appellate review of the government's hybrid theory. The discretion granted to magistrate judges and the continuing absence of hybrid theory analysis by an appellate court leads to the result that "each magistrate judge has effectively become a law unto himself."[188]

178. 18 U.S.C. § 2703(a)–(b) (2006); *see also* Bankston, *supra* note 7, at 632–33.

179. Bankston, *supra* note 7, at 632–33.

180. *Id.* (citing 18 U.S.C. § 2705 (2000)).

181. 18 U.S.C. § 2703(b); *see also* Bankston, *supra* note 7, at 633.

182. 18 U.S.C. § 2703(b); *see also* Bankston, *supra* note 7, at 633 & n.194.

183. Smith, *supra* note 10, at 211.

184. *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005) ("[This opinion] is written in the full expectation and hope that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis.").

185. *See supra* note 15.

186. *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313 (3d Cir. 2010).

187. *Id.* at 319.

188. Smith, *supra* note 10, at 212.

C. Even if an Individual Is Given Notice of the Surveillance and Files a Claim Against the Government, the Claim is Likely to Be Dismissed on Procedural Grounds

In the rare case that an individual does become aware of the electronic surveillance, the individual may still be without recourse. The 2008 Sixth Circuit case *Warshak v. United States*[189] illustrates this point. In 2005, the government obtained ex parte orders, under the authority of the SCA, to search Steven Warshak's e-mails.[190] Warshak did not learn of the orders until roughly a year after they were signed.[191] At that time, "he filed a declaratory judgment action, seeking to invalidate section 2703(d) under the Fourth Amendment, and he moved for a preliminary injunction, seeking to enjoin the government from conducting further *ex parte* email searches."[192] The district court granted his motions, but the Sixth Circuit vacated, holding that Warshak's claims were not ripe for appeal.[193] The court stated: "Warshak's claim epitomizes the kind of dispute that would profit from a concrete factual context."[194] The court refused to infer that factual context from the prior surveillance and, citing only the "possibility" that there would be future ex parte surveillance, also refused to conduct a future-looking review.[195] Without a factual context upon which to analyze the issues, the case would never be "fit for judicial review."[196]

Although the Sixth Circuit did not reach a mootness analysis (because it dismissed the case on ripeness grounds), ex parte surveillance cases are likely to also be moot on appeal. For example, for Warshak's case not to have been moot on appeal, he would have needed to bring it while the surveillance was actually occurring. Of course, this was impossible because he did not learn of the surveillance until a year after it occurred. Thus, for those few individuals who happen to learn that they were subjected to electronic surveillance without the government showing probable cause to obtain authorization for the surveillance, there is still no remedy.

Furthermore, as the circuit court in *Warshak* recognized, "[e]ven outside the case-by-case imperatives of Fourth Amendment decisionmaking, the Supreme Court has expressed increasing skepticism of facial challenges in recent years."[197] This skepticism further insulates the hybrid theory from judicial review.

Another potential issue foreclosing possible remedies is that the government can choose to use the location information derived from suspects' wireless telephones primarily as an investigative tool.[198] Based on the lack of case

---

189. 532 F.3d 521 (6th Cir. 2008).
190. *Id.* at 523.
191. *Id.* at 524.
192. *Id.* at 523.
193. *Id.*
194. *Id.* at 527 (internal citations omitted).
195. *Id.* at 526–27.
196. *Id.* at 526.
197. *Id.* at 529.
198. Interview with Charles R. Pyle, United States Magistrate Judge, Dist. of Ariz., in Tucson, Ariz. (Oct. 2, 2009).

law addressing the Fourth Amendment violations that arguably occur when the government obtains real time cell site location information without showing probable cause, it seems unlikely the government is routinely using the information at trial.[199] Because neither the Pen/Trap Statute nor the SCA require the exclusion of non-content communications obtained in violation of their provisions,[200] defendants must look to the Constitution for any exclusionary remedy. By rarely using the information at trial, the government can effectively repress access to such a remedy, and the Fourth Amendment issues cannot be fleshed out by motions to suppress evidence.[201]

CONCLUSION: POTENTIAL REMEDIES

When the government seeks to use real time cell site location information to track the movement of individuals, the government should be required to show probable cause to obtain court authorization for the surveillance. Although creative, the government's hybrid theory cannot overcome the respective limitations of the Pen/Trap Statute and the SCA. As Judge James K. Bredar of the District of Maryland stated in his 2006 opinion: "Only Congress may authorize courts to order disclosure of prospective cell site information on a showing of less than probable cause, and it is not clear that Congress has done so."[202]

The implications of accepting the false authority of the hybrid theory have not been as widely publicized as the theory's flaws. Particularly, the lack of recourse for individuals subjected to improper surveillance has been often overlooked. The ex parte nature and routine sealing of court orders authorizing the disclosure of cell site location information create a situation in which the parties with the best incentive to appeal orders rarely have knowledge that the surveillance ever took place. Moreover, even if individuals are given notice of the surveillance, the remedies for the potential violations of their Fourth Amendment rights are severely limited. If the individuals learn of the surveillance after its occurrence, it is unlikely any claims they bring against the government will survive procedural dismissal.[203] The government, on the other hand, can tailor its requests for information at the district court level and make calculated decisions to appeal, thus largely controlling the development of the law. While this creates an uncomfortable reality in which the appellate courts are largely paralyzed by the government, it is a reality that can be remedied by legislative or judicial action.

Federal magistrate judges should refuse to sign orders authorizing the disclosure of real time cell site location without the government showing probable cause. Even in the recent Third Circuit opinion, which held that the government may obtain historical cell site location information on a showing of less than probable cause, the court found that magistrates are not *required* to sign orders

---

199. *Id.*

200. Bankston, *supra* note 7, at 631.

201. Interview with Charles R. Pyle, *supra* note 198.

202. *In re* Application of United States for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices of Tel. Nos. [Sealed] & [Sealed], 416 F. Supp. 2d 390, 397 (D. Md. 2006). At the time of this decision, Judge Bredar was serving as a federal magistrate judge.

203. *See* Warshak v. United States, 532 F.3d 521, 523 (6th Cir. 2008).

upon the government meeting the lesser standard.[204] Rather, magistrate judges are permitted to "inquir[e] into the types of information that would actually be disclosed by a cell phone provider in response to the Government's request . . . [and make] a judgment about the possibility that such disclosure would implicate the Fourth Amendment."[205]

Ultimately, it is up to Congress to correct the textual flaws of the Pen/Trap Statute and the SCA to eliminate any inference that the statutes can be combined to create greater authority than either statute has alone.[206] Until Congress takes the initiative to act, however, federal magistrate judges—who are essentially the only line of protection against potential constitutional violations—should require the government to meet the probable cause standard before they authorize disclosure of invasive surveillance information.

204. *In re* Application of United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

205. *Id.* at 317. The court did suggest that the option to require a warrant for the release of historical location information should be "used sparingly." *Id.* at 319.

206. For suggestions on how Congress might revise the statutes, see Bankston, *supra* note 7, at 631–34.