UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN RE APPLICATION OF THE	§	MAGISTRATE NO. H-10-998M
UNITED STATES OF AMERICA	§	MAGISTRATE NO. H-10-990M
FOR HISTORICAL CELL SITE DATA	§	MAGISTRATE NO. H-10-981M

OPINION

In three separate criminal investigations earlier this month, this court denied the Government's request under the Stored Communications Act (SCA) to compel cell phone service providers to produce cell site information for target cell phones. Among other things, each application sought "records or other information pertaining to subscriber(s) or customer(s), including historical cell site information and call detail records (including any two-way radio feature mode) for the sixty (60) days prior to the date the Order is signed by the Court (but not including the contents of communications)."[1] Each application identically defined the requested information as "the antenna tower and sector to which the cell phone sends its signal," specifically including "the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state." In other words, the Government seeks continuous location data to track the target phone over a two month period, whether the phone was in active use or not.

This court has previously granted such requests.[2] However, recent months have

---

[1] Government Applications (redacted), Exs. 1-3, at 2. All exhibits cited in this opinion are in an appendix, docketed separately in each Magistrate case referenced in the caption.

[2] *In re Application of U.S.,* 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) ("By contrast [to prospective cell site data], historical cell site data more comfortably fits the category of transactional records covered by the SCA"). That observation was offered as a matter of statutory interpretation. At the time it was made, my understanding was that providers rarely kept such records (if at all)

brought to light important developments in both technology and caselaw raising serious constitutional doubts about such rulings. Accordingly I denied these requests, but invited the Government if it disagreed to submit a brief to justify its position with appropriate legal and factual support, which it has now done.[3]

Five years ago the first reported decisions on government acquisition of cell site information from telephone companies appeared.[4] The focus of those early decisions was the appropriate legal standard for obtaining prospective location information under the Electronic Communications Privacy Act (ECPA). Thereafter, a handful of decisions addressed the related problem of law enforcement access to historical cell site data collected and maintained by providers over time. A few courts have held that such requests triggered the Fourth Amendment warrant requirement,[5] but most courts to date have granted government access to such information under the SCA, which imposes a less-than-probable cause

---

beyond a week or two. That is apparently no longer the case; Verizon reportedly keeps such records for at least 12 months. Declan McCullagh, *Feds Push for Tracking Cell Phones*, CNET, Feb. 11, 2010, http://news.cnet.com/8301-13578_3-10451518-38.html (last visited Oct. 28, 2010). For the reasons expressed in this opinion, that earlier interpretation of the SCA is now constitutionally impermissible.

[3] Government's brief, No. H-10-998M (Dkt 4).

[4] *See In re Application of U.S.*, 384 F. Supp. 2d 562 (E.D.N.Y. 2005), on reconsideration, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (Orenstein, M.J.); *In re Application of U.S.*, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (Smith, M.J.); *In re Application of U.S.*, 402 F. Supp. 2d 597 (D. Md. 2005) (Bredar, Mag.); *In re Application of U.S.*, 407 F. Supp. 2d 132 (D.D.C. 2005) (Facciola, M.J.); *In re Application of U.S.*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005) (Gorenstein, M.J.).

[5] *See In re Application of U.S.*, 534 F. Supp. 2d 585 (W.D. Pa. 2008) (Lenihan, M.J.), *aff'd* No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sep. 10, 2008) (McVerry, D.J.), *vacated* ___ F.3d ___, 2010 WL 3465170 (3d Cir. Sept. 7, 2010); *In re Application of U.S.*, Nos. 1:06-MC-6, 1:06-MC-7, 2006 WL 1876847 (N.D. Ind. July 5, 2006) (Lee, D.J.).

standard.[6]

Several weeks ago U.S. Magistrate Judge James Orenstein, who authored the very first cell site opinion, suggested in a new opinion[7] that courts re-examine the constitutionality of historical cell site requests in light of recent appellate court decisions, such as that of the District of Columbia Court of Appeals in *United States v. Maynard*.[8] As if to underscore his point, two weeks later the Third Circuit became the first federal appellate court to issue an opinion dealing with government access to historical cell site data.[9] Rather than definitively resolving the Fourth Amendment issue, the court remanded the case to the district court, concluding that the factual record was insufficient to resolve whether such records "could encroach upon . . . citizens' reasonable expectations of privacy regarding their physical movements and locations."[10]

Though significant, the caselaw developments have been outstripped by advancing

---

6 *See* 18 U.S.C. § 2703(d); *In re Application of U.S.*, 509 F. Supp. 2d 76 (D. Mass. 2007) (Stearns, D.J.), *reversing* 509 F. Supp. 2d 64 (D. Mass. 2007) (Alexander, M.J.); *United States v. Suarez-Blanca*, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008) (Baverman, M.J.);*United States v. Benford,* No. 2:09CR86, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010) (Moody, D.J.).

7 *In re Application of U.S.*, No. 10-MJ-00550(JO), 2010 WL 3463132 (E.D.N.Y. Aug. 27, 2010) (holding that historical cell site information is protected by the warrant requirement of the Fourth Amendment).

8 615 F.3d 544 (D.C. Cir. 2010).

9 *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records*, ___ F.3d ___, 2010 WL 3465170 (3d Cir. Sept. 7, 2010).

10 *Id.* at *6.

technology. Recently, committees in both the House and Senate have conducted hearings on proposals to update ECPA, the 1986 statute establishing the regulatory regime governing electronic communications. Expert testimony at those hearings reveals that regulatory and market forces have produced dramatic advances in location technology over the past half-decade. As will be shown, this new technology has altered the legal landscape even more profoundly than the new caselaw.

Mindful of the Third Circuit's admonition to base a Fourth Amendment adjudication on an adequate factual record, the court begins with the following findings of fact. These findings are based on judicially noticed facts derived from material contained in the record appendix, including publicly available industry studies, independent surveys, provider policies, and product specifications. The most significant findings are based on expert testimony recently given at a House Judiciary Subcommittee hearing entitled "ECPA Reform and the Revolution in Location Based Technologies and Services." The purpose of this oversight hearing was not to consider a particular bill, but to educate Congress on the current state of location technology in the telecommunications industry, so that needed reforms to the 1986 statute could be identified, drafted, and debated.[11] Given that such testimony was

---

[11] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 5 (2010) (statement of Rep. Jerrold Nadler, Chairman, Subcomm. on the Constitution, Civil Rights, and Civil Liberties), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF (last visited Oct. 27, 2010) ("Because ECPA inevitably involves the interaction of all these important and complex considerations, we are taking the time through a series of hearings to educate ourselves carefully and fully before beginning to engage in any legislative action. This Subcommittee's exploration of where the appropriate balance may lie with respect to location information must surely include a lesson in

not offered for partisan purposes or to advocate specific legislation, the court finds it particularly appropriate for judicial notice under Rule 201 of the Federal Rules of Evidence.[12]

Findings of Fact

Cell Phone Technology in General

1. Unlike conventional wireline telephones, cellular telephones use radio waves to communicate between the user's handset and the telephone network.[13]

2. Cellular service providers maintain networks of radio base stations ("cell sites") spread throughout their geographic coverage areas.[14]

3. A wireless antenna at each cell site detects the radio signal from the handset, and connects it to the local telephone network, the Internet, or another wireless network.[15]

4. Cell phones periodically identify themselves to a nearby base station as they move about the coverage area, a process called "registration." The registration process is automatic, and occurs whenever the phone is on, without the user's input or control. The registration signal is carried over a channel separate from the channel used to

---

location based technologies and services.").

[12] "A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." FED. R. EVID. 201(b).

[13] Statement of Matt Blaze, Associate Professor of Computer and Information Science, University of Pennsylvania, Ex. 4, at 20.

[14] *Id.*

[15] *Id.*; CTIA website, Ex. 7.

carry the call itself.[16]

5. During a call, if the phone moves nearer to another base station, the call is "handed off" between base stations without interruption.[17]

6. No longer just big three-sided radio towers, base station antennas can be mounted outdoors on roof-tops, building-sides, trees, flagpoles, and church steeples, or indoors in homes and offices. Many are no larger than a conventional stereo speaker.[18]

Wireless Location Technology

7. There are two distinct technological approaches for fixing the location of a cell phone: handset-based (GPS) and network-based (cell site).[19]

8. GPS is the acronym for Global Positioning System, which is comprised of at least 24 satellites constantly orbiting the earth in six low earth orbits.[20]

9. For GPS location, special hardware in a user's handset receives signals from at least four global position satellites, allowing the handset to calculate its latitude and longitude whenever it is in unobstructed satellite range.[21]

---

16 Ex. 4, at 20; DOJ Electronic Surveillance Manual, Ex.19, at 178 n.41.

17 Ex. 4, at 20.

18 CTIA website, Ex.7.

19 Ex. 4, at 20-22.

20 Statement of Michael Amarosa, Senior Vice President for Public Affairs, TruePosition, Inc., Ex. 5, at 38.

21 Ex. 4, at 21; Ex. 5, at 39.

10. Current GPS technology can achieve spatial resolution typically within ten meters.[22]

11. Despite its relative precision, GPS has at least three fundamental drawbacks as a location tool: (a) it is not available for all handset models, especially older models; (b) it works reliably only outdoors, when the handset has an unobstructed view of several GPS satellites in the sky above; and (c) perhaps most significantly, it can be disabled by the user.[23]

12. For these reasons, GPS is neither the most pervasive nor the most generally applicable phone location system, especially for surveillance purposes.[24]

13. For network-based location, the position of the phone is calculated by the network based on data collected and analyzed at the cell site receiving the phone's signals, without explicit assistance from the user or his handset.[25]

14. A variety of techniques may be used for network-based location. The most basic technique is to identify the particular base station (or sector) with which the phone was communicating every time it makes or receives a call and when it moves from one sector to another.[26]

15. The relative precision of cell site location depends on the size of the cell sector. The

---

[22] Ex. 4, at 21.

[23] Ex. 4, at 22; Ex. 5, at 41.

[24] Ex. 4, at 22.

[25] *Id.* at 20-22.

[26] *Id.* at 23.

smaller the sector, the more precise the location fix.[27]

16. In early cellular systems, base stations were placed as far apart as possible to provide maximum coverage. At that time, a sector might cover an area several miles or more in diameter. Today this is true only of sparsely populated, rural areas.[28]

17. Due to a combination of factors, the size of the typical cell sector has been steadily shrinking in recent years.[29]

18. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and antenna.[30]

19. New services such as 3G Internet create similar pressure on the available spectrum bandwidth, again requiring a reduction in the geographic size of sectors.[31]

20. Another factor contributing to smaller sector size is consumer demand for more reliable coverage in areas with unfavorable radio conditions (*e.g.*, elevators), which again requires additional base stations to cover such "dead spots."[32]

21. The number of cellular base stations in the U.S. has tripled over the last decade, and

---

27 *Id.* at 23-24.

28 *Id.* at 24.

29 *Id.*

30 *Id.*

31 *Id.*

32 *Id.* at 25.

the rate of growth is accelerating. By one industry estimate, there are now over 251,000 reported cell sites operating in the United States. There were only 913 the year before ECPA was passed.[33]

22. The trend toward smaller cell sectors has accelerated with the deployment of smaller-scale base stations designed to serve very small areas such as particular floors of buildings, or individual homes and offices.[34]

23. This new generation of cellular base station is generally known as a "microcell," and smaller versions are sometimes referred to as a "picocell"or "femtocell."[35]

24. Microcell technology is increasingly used by many carriers, including AT&T, Verizon, and Sprint. A microcell has a range of 40 feet (12 meters).[36]

25. The effect of this trend toward smaller sectors is that knowing the base station (or sector ID) handling a call is tantamount to knowing the user's location to within a relatively small geographic area. In urban areas and other environments that use microcells, this area can be small enough to identify individual floors and rooms within buildings.[37]

26. The decreasing size of cell sectors is not the only factor making network-based

---

[33] *Id.*; CTIA survey, Ex. 6; CTIA Quick Facts, Ex. 9.

[34] Ex. 4, at 25.

[35] *Id.*

[36] Exs. 10 (AT&T), 11 (Verizon), 12 (Sprint).

[37] Ex. 4, at 25.

location more accurate. New technology allows providers to locate not just the sector in which the phone is located, but also its position within the sector.[38]

27. By correlating the precise time and angle at which a phone's signal arrives at multiple sector base stations, a provider can pinpoint the phone's latitude and longitude to an accuracy within 50 meters or less. Emerging versions of the technology are even more precise.[39]

28. Such enhanced location technologies are commercially available, and many carriers contract with specialized companies that provide "off the shelf" location-based products and system upgrades.[40]

29. Many of these companies were formed in response to directives from Congress and the FCC to develop wireless location technology in order to enhance the nation's emergency response (E-911) system.[41]

Data Collection and Retention

30. Cell location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user.[42]

31. Carriers typically create "call detail records" that include the most accurate location

---

38 *Id.* at 26.

39 *Id.*

40 *Id.*; Ex. 5, at 33-35.

41 Ex. 5, at 33-34.

42 Ex. 4, at 30.

information available to them.[43]

32. Historically, before more advanced location techniques were available, carrier call detail records typically included only the cell sector or base station identifier that handled the call. Today, the base station or sector identifier carries with it more locational precision than it once did.[44]

33. As even more precise location information becomes available, call detail records can now include the user's latitude and longitude along with the sector ID data. Some carriers also store frequently updated, highly precise, location information not just when calls are made or received, but as the device moves around the network.[45]

34. The cost of collecting and storing high resolution location data about every customer has become much cheaper in the last few years. Such information is valuable for network management, marketing, and developing new services. This trend toward greater and more extensive data archives is likely to continue.[46]

35. Some carriers effectively outsource the task of collecting, analyzing, and storing location information to companies offering specialized location technology.[47]

36. One such company installs multiple *auxiliary* receivers (called "Location

---

43 *Id.* at 27.

44 *Id.*

45 *Id.*

46 *Id.* at 27-28.

47 Ex. 5, at 44-45.

Measurement Units", or LMUs) on existing cell towers and base stations to enhance location accuracy. These auxiliary receivers are very accurately time-synchronized to each other, and very sensitive; at any given moment, a single handset may be in communication with 30 or more LMUs.[48]

37. This same company has deployed over 100,000 LMU's.[49]

38. The company not only transmits this detailed location information to the carrier, it can also manage and analyze historic location and calling activity data. Such data can also be organized and aggregated to reflect current user activities, mobile events, and interaction with other devices.[50]

39. Most carrier systems use a variety of large and small sector configurations. A mobile user, in the course of her daily movements, will periodically move in and out of large and small sectors. The locational precision of cell sector data recording those movements will vary widely over the course of a given day, from relatively less to relatively very precise.[51]

40. Neither the user nor the carrier can predict how precise the next location data will be. For a typical user, over time, some of that data will likely have locational precision

---

48 *Id.* at 40.

49 *Id.*

50 *Id.* at 44.

51 Ex. 4, at 28.

similar to that of GPS.[52]

41. Given these advances in technology, it is no longer valid to assume that network cell sector records will yield only an approximate user location.[53]

42. As cellular network technology evolves, the traditional distinction between "high accuracy" GPS tracking and "low accuracy" cell site tracking is increasingly obsolete, and will soon be effectively meaningless.[54]

Cell Phone Use Statistics

43. Today there are more than 285 million active wireless subscriber accounts in the United States. Many households no longer have traditional "landline" telephone service, opting instead for cellular phones carried by each family member.[55]

44. Cell phones are frequently used in the home or in other places not open to public view: one study shows that at least 52% of cell phone calls are made indoors;[56] another study indicates that two out of three adults sleep with their cell phone nearby.[57]

45. In 1999, the number of reported wireless minutes of use was less than 200 billion. A

---

52 *Id.* at 28-29.

53 *Id.* at 29.

54 *Id.*

55 Ex. 4, at 19.

56 Exhibit 5, at 48 (citing J.D. Power's 2009 Wireless Call Quality Performance Study—Volume 1).

57 Pew Research Center Study, Ex. 13.

decade later, the number has grown to more than 2.2 *trillion* minutes.[58]

46. Over the same decade, the annual number of text messages has jumped to 1.56 trillion.[59]

47. According to a 2008 Nielsen survey, the average U.S. cell phone user made or received 204 voice calls every month.[60] A 2010 Pew Research study of adult cell phone use show that the median number of voice calls for a typical user is 5 per day, while the average (mean) is 13.1calls/day. This study also shows that African American and Hispanic cell users make more calls (and texts) on average than their white counterparts.[61]

48. Similar patterns are reflected in cell phone texting. The 2008 Nielsen survey reported the average cell phone user made or received 357 text messages a month.[62] According to the 2010 Pew Research study, adults send and receive a median of 10 texts daily; the average (mean) is 39.1 texts/day. Both figures are more than double the levels reported by Pew just 8 months earlier in September 2009. Teen use of text messaging is substantially heavier: the teen median level is 50 texts daily, and the mean is

---

58 Ex. 6.

59 *Id.*

60 Neilsen Wire (Sept. 22, 2008), Ex. 14.

61 Ex. 13, at 3, 23.

62 Ex. 14.

112.4.[63]

49. Based on these numbers, even if limited to the beginning and end of actual phone calls and text messages, cell site data for a typical adult user will reveal between 20 and 55 location points a day. This data is sufficient to plot the target's movements hour by hour for the duration of the 60 day period covered by the government's request.[64]

50. If registration data were also collected by the provider and made available, as the Government has requested, such records would track the user on a minute by minute basis, compiling a continuous log of his life, awake and asleep, for a two month period.

Conclusions of Law

A. Under Current Location Technology, Cell Site Information Reveals Non-Public Information About Constitutionally Protected Spaces

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." At its core, the Fourth Amendment safeguards "the right of a man to retreat into his own home and there be free from unreasonable government intrusion." *Silverman v. United States,* 365 U.S. 505,

---

63 Ex. 13, at 23.

64 The Government has offered a one page document described as a "redacted sample of historical cell site information," produced by T-Mobile in response to an unspecified order issued October 6, 2010 and including some calls from September 2010. Ex. 17 (H-10-998M, Dkt 4-1). The document has 50 location points, but does not indicate what day(s) the calls were made, or whether this represents all cell site data produced in response to the order. Nor is there any indication of the size of the listed cell sectors, or the locational precision of the data.

511 (1961). "With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Kyllo v. United States,* 533 U.S. 27, 31 (2001). A "search" occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. *United States v. Jacobsen,* 466 U.S. 109, 113 (1984); *see also Katz v. United States*, 389 U.S. 347, 353 (1967).

The refinements in location-based technology detailed in the findings of fact have decisive Fourth Amendment consequences. Perhaps most significantly, they bring cell site location data squarely within the protective ambit of *United States v. Karo,* 468 U.S. 705 (1984).

Karo considered whether Fourth Amendment rights were violated by law enforcement monitoring of an electronic tracking device known as a "beeper."[65] Law enforcement had placed the beeper inside a can of ether to be used to extract cocaine from clothing imported by drug dealers, and then monitored the beeper's movements over a period of several months. At one point the beeper was detected near a commercial storage warehouse; however, the beeper equipment was too imprecise to pinpoint a specific locker, and so such monitoring was held not to intrude upon the suspects' expectation of privacy in their own storage locker. *Id.* at 720 n.6. On another occasion, however, the beeper was monitored while inside a

---

[65] A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver. *United States v. Knotts,* 460 U.S. 276, 277 (1983). The current generation of tracking device beepers are monitored by radio signals transmitted via the very same cell towers used to carry wireless phone signals. *See In re Application of U.S.*, 396 F. Supp. 2d 747, 754 (S.D. Tex. 2005) ("Given this convergence in technology, the distinction between cell site data and information gathered by a tracking device has practically vanished.").

private residence, a place not open to visual surveillance. The Court held that such warrantless monitoring violated the Fourth Amendment, because it revealed "that the beeper was inside the house, a fact that could not have been visually verified." *Id.* at 715.

Like the beeper signal from the residence in *Karo*, cell site information permits the government "to determine by means of an electronic device . . . whether a particular article – or a person, for that matter – is in an individual's home at a particular time." *Id.* at 716. Over the course of two months, it is inevitable that dozens if not hundreds of calls and text messages of a typical user will be sent from home, office, or other place out of public view. Each of these calls and messages will generate network-based location information, much of it as precise as GPS data.[66] Even if no calls or texts were ever made, the phone's presence within the home at a given time would likely be revealed by the automatic registration process.[67] This is precisely the type of information that *Karo* held subject to Fourth Amendment protection; it makes no difference that the electronic device employed is more sophisticated than a traditional beeper.[68]

---

[66] Findings of Fact 14, 42.

[67] This is one of the factors which distinguishes cell site data from the phone numbers dialed in *Smith v. Maryland,* which were held unprotected by the Fourth Amendment. Unlike a wireline phone in a fixed location such as a residence, a cell phone accompanies its user throughout the day, revealing when the user leaves the house and when he returns. Also, because each member of a household is likely to have her own phone, cell site data is more likely to reveal which household member made a particular call from the residence.

[68] Of course, the records sought here were not the product of law enforcement surveillance, but were gathered and maintained by the providers in the course of their business. Based on this distinction, the Government argues that the third party doctrine of *U.S. v. Miller* applies, and therefore its request is not a "search" for purposes of the Fourth Amendment. This contention is considered (and rejected) in Part C below.

Before the Third Circuit, the Government argued that cell site location data no more precise than 200 feet was insufficient to trigger Fourth Amendment protection.[69] By the same token, when seeking to acquire GPS or similarly precise location data (often referred to as "E-911 data") from this court, the Government has regularly proceeded by way of a Rule 41 warrant, a tacit concession that such data would reveal facts about a constitutionally protected space.[70] Now that cell site technology permits a location fix approaching the precision of GPS – *e.g.*, microcells with a radius of 40 feet[71] – the technology undergirding the Government's policy has gone the way of VHS and Betamax.

Likewise, court decisions allowing the Government to compel cell site data without a probable cause warrant were based on yesteryear's assumption that cell site data (especially from a single tower) could locate users only imprecisely.[72] Given that network-based technology is now capable of isolating a mobile phone user to a particular floor or room

---

69 Brief for the United States at 34-35, 2009 WL 3866618 (Feb. 13, 2009). This proposition is questionable in itself. Even in areas where houses and cell towers are few and far between, law enforcement may reliably pinpoint a target's exact location with little more than a known address or direct observation. *See, e.g.,* the unfortunate case of Mr. Nesbitt of Harlow New Town, depicted at www.youtube.com/watch?v=ltmMJntSfQI (last visited Oct. 29, 2010).

70 Email from Mark Eckenwiler, Associate Director, Office of Enforcement Operations, Criminal Division, United States Department of Justice, to unknown recipients (Nov. 16, 2007, 14:19), *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_crm200800549f_20080822.pdf (last visited Oct. 28, 2010) ("We continue to believe that the most appropriate legal mechanism [for GPS or similarly precise location data] is a Rule 41 warrant.").

71 Finding of Fact 24.

72 *See, e.g., United States v. Suarez-Blanca,* No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156 *11 (N.D. Ga. Apr. 21, 2008) (historical cell site information); *In re Application of U.S.,* 411 F. Supp. 2d 678, 681-83 (W.D. La. 2006) (prospective cell site information).

within a building, and that such increasingly precise "call detail records" are now kept by providers, the continuing vitality of those decisions must be doubted (with all due respect).

Even if an exact latitude and longitude is not yet ascertainable or recorded for every single mobile call, network technology is inevitably headed there.[73] As the Supreme Court observed in *Kyllo v. United States* regarding the ongoing research and development of radar surveillance devices:

> While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or development.

533 U.S. 27, 36 (2001). Like the thermal imaging devices in *Kyllo,* the cellular location technology in use or development today crosses the "firm but also bright" Fourth Amendment line that the Supreme Court has drawn at the entrance to the house. *Id.* at 40. Accordingly, the cell site records generated by that technology are subject to constitutional protection.

B. Historical Cell Site Records Are Subject to Fourth Amendment Protection under the Prolonged Surveillance Doctrine of *United States v. Maynard*

It is true that cell site records for a single day may not always reveal particularly intimate details about the user's private life but merely that the user's cell phone (like the *Karo* beeper) was present in the home at a particular time. Nevertheless, as Justice Scalia has observed, "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes." *Kyllo,* 533 U.S. at 37 (emphasis in original).

---

[73] Finding of Fact 42.

In this case, the records sought by the Government are likely far more intrusive – not a single snapshot at a point in time, but a continuous reality TV show, exposing two months' worth of a person's movements, activities, and associations in relentless detail.

In his decision denying warrantless access to historical cell site information, Judge Orenstein relied most heavily on the recent decision of the Court of Appeals for the District of Columbia in *United States v. Maynard,* 615 F.3d 544 (D.C. Cir. 2010). In light of the technological developments noted above, reliance on the *Maynard* precedent is not essential to the ruling here. Even so, *Maynard*'s treatment of month-long GPS surveillance is instructive, and provides additional support and alternative grounds for this decision.

Police in *Maynard* tracked the movements of a suspected drug dealer 24 hours a day for four weeks with a GPS device they had installed on his Jeep without a warrant. The Government used the resulting pattern of those movements – "not just the location of a particular 'stash house' or Jones's movements on any one trip or even day"[74] – as evidence of drug trafficking conspiracy. Jones argued that the month-long warrantless tracking of his Jeep violated the Fourth Amendment prohibition of "unreasonable searches," and the D.C. Circuit agreed.

The *Maynard* court began by distinguishing *United States v. Knotts*, which had held that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U.S. 276, 281

---

[74] 615 F.3d at 562 n.*.

(1983). The police in *Knotts* had monitored a beeper placed in a five-gallon container while it was driven in a car 100 miles over public roads to a cabin in rural Wisconsin. Because the defendant by driving on public roads had "voluntarily conveyed to anyone who wanted to look" his progress and route, the Court held the beeper monitoring had violated no reasonable expectation of privacy, and hence was not a search under the Fourth Amendment. *Id.*

As *Maynard* correctly notes, the *Knotts* opinion expressly reserved the question whether a warrant would be required for prolonged or twenty-four hour surveillance.[75] The D.C. Circuit held that *Knotts* was not controlling, because the tracking was not limited to a single trip from one place to another, but instead covered "Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place." 615 F.3d at 558. The court persuasively elaborates why prolonged location surveillance is different:

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movement's can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals

---

[75] 615 F.3d at 556-58 ("[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." (quoting *Knotts,* 460 U.S. at 283-84)).

> or political groups– and not just one such fact about a person, but all such facts.

615 F.3d at 562 (footnote omitted).[76] The court concluded that an individual has a legitimate expectation of privacy regarding the "intimate picture of his life" revealed by prolonged surveillance, citing various state privacy laws as well as the "considered judgments of every court to which the issue has been squarely presented."[77]

As Judge Orenstein observed, there are certain differences between the real-time GPS tracking in *Maynard* and the historical cell site records at issue here, but none support a different result. The temporal distinction between prospective and historical location tracking is not compelling, because the degree of invasiveness is the same, whether the tracking covers the previous 60 days or the next. In Judge Orenstein's words, "The picture of Tyshawn Augustus's life the government seeks to obtain is no less intimate simply because it has already been painted."[78] Nor does it matter, for Fourth Amendment purposes, that the information sought was neither created nor maintained at the direction of law enforcement.

---

[76] Judge Ginsburg's opinion echoes the same concerns over locational privacy which led Congress to pass the WCSPA in 1999. *See* Part C, *infra*.

[77] 615 F.3d at 564-65. *See People v. Weaver*, 909 N.E.2d 1195, 1203 (N.Y. 2009) ("the installation and use of a GPS device to monitor an individual's whereabouts requires a warrant supported by probable cause"); *State v. Jackson,* 76 P.3d 217, 224 (Wash. 2003) (*en banc*) ("use of a GPS device on a private vehicle involves a search and seizure" under state constitution). Although some federal circuits have held the use of a GPS device is not a search, the D.C. Circuit accurately noted that those courts did not consider the distinction drawn in *Knotts* between short-term and prolonged surveillance. 615 F.3d at 557-58, 564. *See United States v. Marquez,* 605 F.3d 604 (10th Cir. 2010);*United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010); *United States v. Garcia,* 474 F.3d 994 (7th Cir. 2007).

[78] 2010 WL 3463132, at *6 (E.D.N.Y. Aug. 27, 2010).

See United States v. Miller, 425 U.S. 435, 443 (1976) ("This [Fourth Amendment] analysis is not changed by the mandate of the Bank Secrecy Act that records of depositors' transactions be maintained by banks"). The fact that the records are presently in the hands of a third party might be dispositive if they had been "voluntarily conveyed" to the provider by the customer, but, as explained in the next section, that is not true of cell site tracking data.

In several respects, the historical cell site records sought here are more invasive than the GPS data revealed in *Maynard.* The duration and volume of information sought is more than doubled – 60 days as opposed to 28 days of movement. As we have found, the level of detail provided by cell site technology now approaches that of GPS, and its reliability in obtaining a location fix actually exceeds that of GPS.[79] Moreover, as Judge Orenstein points out, cell phone tracking is likely more revealing than a GPS device attached to a car, because the cell phone is carried on the person.[80] It will also inevitably be more intrusive, because the phone can be monitored indoors where the expectation of privacy is greatest. By contrast, the GPS device in *Maynard* revealed no information about the interior of a home or other constitutionally protected space.

Finally, the Government's brief suggests that, as in *Maynard*, Fourth Amendment concerns are best addressed at a suppression hearing, after the search has taken place. But

---

[79] *See* Findings of Fact 11, 41.

[80] 2010 WL 3463132, *10 (E.D.N.Y. Aug. 27, 2010).

magistrate judges do not have the luxury of retrospective adjudication, waiting until a search occurs to decide whether a search warrant was required. If asked to issue an order that in our considered view violates the constitution, our sworn duty is to deny that application. Sometimes, the law is uncertain, because the Supreme Court has not definitively ruled. In such cases it is especially important for magistrate judges to explain their reasons on the record, giving affected parties (including the Government) the right to seek appellate review and correction, if necessary, by the Supreme Court. Murky areas of law like the ECPA remain murky decades after passage for two principal reasons – a dearth of reported district court decisions to generate appellate review, and a regime of sealing and gag orders to conceal court rulings from the general public and affected parties.[81]

For all these reasons, I join Judge Orenstein in holding that *Maynard*'s prolonged surveillance doctrine precludes the Government from obtaining two months of cell phone tracking data without a warrant.

C. Because the Government Has Not Shown That the Location Data Sought Was Voluntarily Conveyed by the User, *Smith v. Maryland* Does Not Eliminate a Legitimate Expectation of Privacy

The Government urges that no Fourth Amendment interest is implicated here, because it is merely seeking the production of cell site data voluntarily conveyed by the target phone

---

[81] *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 76-77 (2010) (statement of Judge Stephen Wm. Smith, United States Magistrate Judge, Southern District of Texas), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF (last visited Oct. 27, 2010).

user to the provider. As the Supreme Court stated in *Katz v. United States*, "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." 389 U.S. at 351 (1967). In *United States v. Miller*, the Court found no legitimate expectation of privacy in bank checks, deposit slips, and financial statements, because they "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." 425 U.S. 435, 442 (1976). Perhaps the most directly relevant application of this doctrine is *Smith v. Maryland,* 442 U.S. 735 (1979), where the Court found a telephone user had no legitimate privacy interest in phone numbers he dialed, because

> [w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.

Id. at 744.

As with any Fourth Amendment claim involving records, a court "must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Miller,* 425 U.S. at 442; *see also Smith*, 442 U.S. at 741("[I]t is important to begin by specifying precisely the nature of the state activity that is challenged."). The records at issue here are "historical cell site information and call detail information" for the target phone "for the sixty (60) days prior to the date the Order is signed by the Court."[82] As defined in the Government's applications,

---

[82] The full definitions of "cell site information" and "call detail records" in the applications are as follows:

this information includes "the cellsite/sectors used by the mobile telephone to obtain service for a call or *when in an idle state*."[83] Clearly, these requests seek the phone's location not only at the beginning and end of calls, but also "registration" information as the phone moves about the network. In other words, the Government is asking for all available records tracking the phone's continuous location and movement during a two month period.

The first thing to note about this tracking data is that, although perhaps generated in the ordinary course of the provider's business, it is not a proprietary business record subject to unfettered corporate control, such as a marketing plan or an expense report or a soft drink formula. In 1999, Congress passed the Wireless Communication and Public Safety Act (WCPSA),[84] which amended the Telecommunications Act to place limits on the carrier's use or disclosure of a cell phone user's location information. The existing statute obliged the

---

> A cell phone must send a radio signal to an antenna tower which, in turn, is connected to the provider's network. The area covered by the tower varies depending on the population density of the area. This area is often divided into thirds – 120 degree sectors. "Cell site information" as used in this application refers to the antenna tower and sector to which the cell phone sends its signal. This includes the physical location and/or address of the cellular tower and identification of the particular sector of the tower receiving the signal. Exs. 1-3, at n.3.
>
> "Call detail records" are similar to toll records (i.e. historical telephone records of telephone activity, usually listing outgoing calls and date, time, and duration of each call), which are made and retained in the ordinary course of business. However, "call detail records" is the term used when referring to toll records of mobile telephones rather than hardline telephones. Unlike toll records, however, call detail records also include a record of incoming calls and the cellsite/sector(s) used by the mobile telephone to obtain service for a call or when in an idle state. Exs. 1-3, at n.4.

[83] *See, e.g.*, Ex.1, at 2 n.4.(emphasis added)

[84] Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999), codified at 47 U.S.C. § 222(f).

telecommunications carrier to protect the confidentiality of "customer proprietary network information" (CPNI), that is, information about a customer's use of the service that was made available to the carrier by the customer solely by virtue of the carrier-customer relationship. 47 U.S.C. § 222(f)(1) (1996). In order to enhance privacy protection for wireless consumers, the new statute amended the definition of CPNI to include "location," and added the following section:

> **(f) Authority to use wireless location information**
>
> For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—
>
> (1) call location information concerning the user of a commercial mobile service . . . or the user of an IP-enabled voice service . . ., other than in accordance with subsection (d)(4) of this section. . .

47 U.S.C. § 222(f)(1999). The privacy concerns animating this legislation were well articulated by one of the bill's sponsors on the House floor:

> There is no question that information-rich location systems that do wonders to help save lives on our Nation's roadways also pose significant risks for compromising personal privacy. This is because the technology also avails wireless companies of the ability to locate and track individual's movements throughout society, where you go for your lunch break; where you drive on the weekends; the places you visit during the course of a week is your business. It is your private business, not information that wireless companies ought to collect, monitor, disclose, or use without one's approval. . . .
>
> Wherever your cell phone goes becomes a monitor of all of your activities.

145 Cong. Rec. H9858-01, at H9860 (daily ed. Oct. 12, 1999) (statement by Rep. Edward

Markey). Other members expressed similar privacy concerns.[85]

Of course, the statute did not place location information beyond the reach of law enforcement, and its privacy protections are not conclusive on whether a warrant is necessary to compel its production.[86] Nevertheless, an act of Congress affecting proprietary interest in a thing is undeniably relevant to the legitimate-expectation-of-privacy inquiry.[87] The WCPSA operates as a type of federal property law, balancing the interests of cell phone users and carriers in personal data generated as a result of providing telecommunication service. The fact that WCPSA imposes heightened privacy protection for a customer's call location information is highly relevant, especially given that the topic of wireless phone location is specifically mentioned in only one other federal statute, CALEA, which forbids its

---

[85] *See*, *e.g.*, 145 Cong. Rec. H9858-01, at H9860 (daily ed. Oct. 12, 1999) (statement by Rep. Wilburt Tauzin) ("[The privacy provision] protects us from Government knowing where you are going and what you are doing in your life"); H145 Cong. Rec. H9858-01, at H9862 (daily ed. Oct. 12, 1999) (statement by Rep. Gene Green) ("we do not want Big Brother looking over our shoulders"); 145 Cong. Rec. H9858-01, at H9863 (daily ed. Oct. 12, 1999) (statement by Rep. Thomas Bliley) ("It is not appropriate to let government or commercial parties collect such information or keep tabs on the exact location of individual subscribers. S. 800 will ensure that such call location information is not disclosed without the authorization of the user, except in emergency situations, and only to specific personnel.").

[86] *See City of Ontario v. Quon,* 130 S. Ct. 2619, 2632 (2010) ("Respondents point to no authority for the proposition that the existence of statutory protection renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise.").

[87] *See, e.g., United States v. Jacobsen*, 466 U.S. 109, 123 (1984) ("Congress has decided . . . to treat the interest in 'privately' possessing cocaine as illegitimate; thus government conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest."); *Rakas v. Illinois,* 439 U.S. 128, 143 n.12 (1978) ("Legitimate expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."); *Miller,* 425 U.S. at 442-43 ("The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act.").

acquisition by law enforcement under the very relaxed standard for pen registers.[88] At the very least, the WCPSA ties certain "strings" to call location data, pulling them out of the category of ordinary business records subject to a carrier's exclusive dominion and control.

Contrary to the Government's claim, the WCPSA does not "by its terms allow[] compelled disclosure pursuant to the SCA." Government brief, at 16. The statute does not mention the SCA. It merely recognizes an exception to its disclosure restrictions "as required by law." 47 U.S.C. § 222(c)(1). This language is perfectly consistent with a Fourth Amendment warrant requirement.

With this in mind, we return to the crux of the Government's argument – that cell site location information has been "voluntarily conveyed" by the cell phone user to the carrier, and thus *Miller* and *Smith* preclude Fourth Amendment protection. This contention has been directly addressed by two appellate courts to date, and both have rejected the claim. In *United States v. Forest*,[89] the Sixth Circuit considered a drug dealer's claim to suppress the cell site data used to convict him. Law enforcement had dialed the defendant's phone without allowing it to ring, and the resulting cell site data was used to track his movements while driving on a public highway. The court was persuaded that *Smith* did not apply because the

---

88 *See* 47 U.S.C. § 1002(a)(2) ("information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . shall not include any information that may disclose the physical location of the subscriber").

89 355 F.3d 942 (6th Cir.), *cert. denied* 545 U.S. 856 (2004). The Supreme Court subsequently granted certiorari on a sentencing issue for one of the two co-defendants, vacating the judgment and remanding "for further consideration in light of *United States v. Booker*." *Garner v. United States,* 543 U.S. 1100, 124 S. Ct. 1050, 1051 (2005).

defendant had not voluntarily conveyed his cell site data to anyone; the agent, not the defendant, had dialed the number which caused the phone to send out signals.[90] By necessary implication, in order to "voluntarily convey" location information under *Smith,* the user must do more than merely turn the phone on.

More recently, the Third Circuit went a step further, declaring that a cell phone user does not voluntarily convey location information by making or receiving a call. Rejecting the Government's analogy to the phone numbers dialed in *Smith*, the court explained:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." EFF Br. at 21.

2010 WL 3465170 at *11 (emphasis in original). This court reached a similar conclusion in its 2005 cell site decision.[91] Although not all district courts have followed our lead on this point,[92] nothing in those decisions or the Government's brief convincingly challenges that proposition.

Unlike the bank records in *Miller* or the phone numbers dialed in *Smith,* cell site data

---

[90] 355 F.3d at 951. The Sixth Circuit ultimately rejected the defendant's constitutional claim on the narrower ground that the cell site data merely revealed his location on public highways, where there is no legitimate expectation of privacy under *United States v. Knotts*, 460 U.S. 276, 281 (1983).

[91] 396 F. Supp. 2d at 756-57.

[92] *See, e.g., Suarez-Blanca,* 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008).

is neither tangible nor visible to a cell phone user. When a user turns on the phone and makes a call, she is not required to enter her own zip code, area code, or other location identifier. None of the digits pressed reveal her own location. Cell site data is generated automatically by the network, conveyed to the provider not by human hands, but by invisible radio signal. Thus, unlike in *Miller* or *Smith,* where the information at issue was unquestionably conveyed by the defendant to a third party, a cell phone user may well have no reason to suspect that her location was exposed to anyone. The assumption of risk theory espoused by *Miller* and *Smith* necessarily entails a knowing or voluntary act of disclosure; the Government has cited no case (and the court has found none) where unknowing, inadvertent disclosure of information by a defendant thereby precluded Fourth Amendment protection of that information.

One might argue that all cell phone users *ought* to know that their precise location will be conveyed to the provider because it is necessary to connect the call – otherwise the call could not be made. But that premise is simply untrue. As recent congressional testimony shows,[93] before the advent of GPS and the current generation of network-based technology, it was not possible to locate cell phone users with any degree of precision.[94] For that very reason, the Federal Communications Commission in 1997 issued final "Enhanced 911" (E-911) rules requiring providers to upgrade their systems to enable emergency responders to

---

93 Ex. 5, at 35-36.

94 *See In re Revision of the Comm'n's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Sys.*, 15 FCC Rcd. 17442, 17462 (2000), Ex. 18.

locate mobile units making emergency 911 calls for rescue or assistance.[95] Thus, even a tech-savvy cell phone user would not expect that anything more than an approximate location, such as his general neighborhood or area code, would be necessary for the network to complete a call.

The T-Mobile privacy policy tendered by the Government says no more than that: "Our network detects your device's *approximate* location whenever it is turned on (subject to coverage limitations)."[96] Elsewhere the policy informs customers that call details and call location information are CPNI and reassures them that "Under federal law, you have a right, and we have a duty, to protect the confidentiality of CPNI and we have adopted policies and procedures designed to ensure compliance with those rules."[97] Included in the record appendix are the terms of use for Metro PCS,[98] the service provider for one of the other target phones, which describe arguably different policies and practices concerning the collection and retention of location information. Parsing the differences among the particular record-keeping practices of various providers would do little to advance the constitutional inquiry, however. As the Supreme Court wryly observed in *Smith v. Maryland*: "We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here)

---

[95] The implementation date for compliance has been repeatedly delayed, and is currently 2012. *See* 47 C.F.R. § 20.18(h)(1)(2008).

[96] Ex. 16 (emphasis added).

[97] *Id.* at 4.

[98] Ex. 15.

the pattern of protection would be dictated by billing practices of a private corporation."[99]

Of course, the tech-savvy user may now understand that there is a risk that the provider can calculate and record his location and movements very precisely. But the bare possibility of disclosure by a third party cannot by itself dispel all expectation of privacy. Otherwise, nothing would be left of *Katz*, because it was surely possible in 1967 for the phone company to wiretap and disclose a private conversation in a public phone booth. Similarly, it is possible that a carrier may open and inspect a letter or sealed package, but that risk alone does not eliminate the legitimate expectation of privacy in such effects. *United States v. Jacobsen,* 466 U.S. 109, 114 (1984); *Ex parte Jackson,* 96 U.S. 727, 733 (1877).

In sum, *Miller* and *Smith* do not permit warrantless law enforcement access to all historical cell site data, because the user has not "knowingly exposed" or "voluntarily conveyed" that information to the provider, as those phrases are ordinarily understood. Historical cell site data are not ordinary business records of the providers. Congress has placed limits on the use and disclosure of call location information absent customer approval, and specifically forbade implying such approval based on mere use of the phone. Thus, consumers are not forced to sacrifice locational privacy as the price of using cell phones. This judgment of Congress may not be conclusive as to Fourth Amendment protection, but neither should it be ignored, especially when, as in the case of cell site data, it jibes

---

[99] 442 U.S. at 745.

comfortably with Fourth Amendment precedent.[100]

Conclusion

The "inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year."[101] In 1789 it was inconceivable that every peripatetic step of a citizen's life could be monitored, recorded, and revealed to the government. For a cell phone user born in 1984, however, it is conceivable that every movement of his adult life can be imperceptibly captured, compiled, and retrieved from a digital dossier somewhere in a computer cloud. Now as then, the Fourth Amendment remains our polestar.

It is true that the Government's warrantless requests are here limited to 60 days, but the logic of its position admits no temporal restraint. Two months' worth of hourly tracking data will inevitably reveal a rich slice of the user's life, activities, and associations; the D.C. Circuit has required a search warrant for half as much. If the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera.

For these reasons, I arrive by a slightly different path at the same destination as my colleagues from Pennsylvania, New York, Massachusetts, Indiana, and Austin, Texas.

---

[100] Of course, the situation is different when a phone customer uses or subscribes to a location-based service, and for that purpose knowingly transmits his GPS position to the service provider. The Government's requests are not limited to (and do not even mention) such records here. Query whether such a transmission by the user would be classified as communications content, and therefore not obtainable under the lesser standard of a 2703(d) order?

[101] 396 F. Supp. 2d at 755.

Compelled warrantless disclosure of cell site data violates the Fourth Amendment under the separate authorities of *Karo* and *Maynard*. Accordingly, the Government's requests for that information under the SCA are denied.

Signed at Houston, Texas, on October 29, 2010.

Stephen Wm Smith
United States Magistrate Judge