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

---

[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)

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.

Government's brief, No. H0000 1.00000 0.0000 0.0000D(ov)Tj6v18.6400 0.0000 TD(S)T0 0 0.0000 TD(h,)Tj1

[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*, No. 10-MJ-00550(JO), 2

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

---

[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

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.

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,

---

[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.

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

[34] Ex. 4, at 25.

[35] *Id.*

Exs. 10 (AT&T), 118.1

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.

[52] *Id.* at 28-29.

[53] *Id.* at 29.

[54] *Id.*

Ex.

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

46.

---

58 Ex. 6.

59 *Id.*

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

61 Ex. 13, at 3, 23.

62 Ex. 14.

[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

[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

[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.00000 0.00000 1.00000 0.coown

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.

(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 quest

---

[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)).

did n

> 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 resnc0000 TD(e pi)Tjp.0000 TD(q)Tj6h0000 1.00000 0.000(4.)Tj12.3600 0.0000

---

[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* reveale ce[illegible]

[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 recor

---

[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).

telecom

[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.").

See City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) ("Respondents point to

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 o

[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).

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 polest

---

[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 *O.cr*