UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

IN RE SMARTPHONE GEOLOCATION DATA APPLICATION

MEMORANDUM AND ORDER
13-MJ-242 (GRB)

----------X

Appearances:

Loretta E. Lynch
United States Attorney
by: Allen Bode, AUSA,
Central Islip, NY

GARY R. BROWN, United States Magistrate Judge:

The Government obtained an arrest warrant for a physician based on a showing that he had issued thousands of prescriptions for highly addictive controlled substances to addicts and drug dealers in exchange for cash, continuing these illegal and dangerous practices even after learning of a DEA investigation into his activities and surrender of his controlled substances registration. After the physician expressly refused to surrender or provide information about his whereabouts, the Government filed the instant application for prospective geolocation data relating to the cell phone believed to be used by the physician. After the Court granted this authorization, the Government used the cell site data to apprehend the defendant and, upon his capture, uncovered evidence reflecting defendant's effort to flee the country to avoid prosecution.

This Memorandum and Order memorializes the rationale for authorizing access to prospective geolocation data for the defendant's cellular phone in these circumstances. This determination rests on two grounds. First, the Court is authorized to issue a search warrant where, as here, the Government demonstrates probable cause to believe that the information sought will aid in the apprehension of an individual subject to an arrest warrant. Second, given

the ubiquity and celebrity of geolocation technologies, an individual has no legitimate expectation of privacy in the prospective location of a cellular telephone where that individual has failed to protect his privacy by taking the simple expedient of powering it off. Thus, in these circumstances, the Government may seek a search warrant for prospective geolocation data or, in the alternative, may obtain an authorization order under the Electronic Communications Privacy Act.

BACKGROUND

The Arrest Warrant

On March 18, 2013, the United States Attorney presented an affidavit seeking the issuance of an arrest warrant for Gracia L. Mayard ("Dr. Mayard" or "defendant"), a medical doctor, for violation of 18 U.S.C. § 846. *See* Affidavit in Support of an Arrest Warrant, Docket Entry ("DE") [1], *United States v. Mayard*, 13-MJ-238 (E.D.N.Y. Mar. 18, 2013) ("Arrest Affidavit"). That affidavit sets forth, in relevant part, the following facts:

Oxycodone is a highly-addictive medical painkiller, which can be misused to produce a heroin-like high. *Id.* ¶ 9. Dr. Mayard became the subject of a Drug Enforcement Administration ("DEA") investigation triggered by his prescription of an unusually large number of oxycodone pills. *Id.* ¶ 10. On February 7, 2013, as part of this investigation, DEA agents attempted to contact Dr. Mayard at his home and office located in Cambria Heights, New York. *Id.* ¶ 11. After unsuccessfully attempting to conceal himself from the agents, Dr. Mayard led the agents into his "exam room," a space that appeared both unused and ill-equipped to conduct medical examinations. *Id.* ¶¶ 12-13. Dr. Mayard reported to the agents that "I see 20 to 50 patients a day" in the office. *Id.* ¶ 14. When asked about his seemingly excessive prescription of oxycodone, Dr. Mayard advised that he "thought the limit was 10 prescriptions a day" but that ultimately "what happens to the oxycodone after I write the prescription is not my concern." *Id.*

He compared himself to "a person that sells guns [who] cannot control what happens after he sells a gun." *Id.* Agents requested that Dr. Mayard voluntarily surrender his DEA registration to prescribe controlled substances, to which he agreed, though Dr. Mayard requested to post-date the form because he had already written 20 to 30 post-dated prescriptions through the month of February. *Id.* ¶ 15. The DEA denied the request, and Mayard surrendered his registration effective that day. *Id.*

Dr. Mayard maintained patient files consisting mainly of copies of driver's licenses and oxycodone prescriptions (including post-dated prescriptions), with little or no additional information about the purported patients, many of which were stored in the back seat of his car. *Id.* ¶ 19-20. In interviews, several of Dr. Mayard's patients indicated that they had never met him. *Id.* ¶¶ 21-23. One recipient obtained a prescription from an acquaintance to whom she paid $300 to fill the prescription at a pharmacy in Queens, New York. *Id.* ¶ 22. Another patient visited Dr. Mayard who, without performing an examination, wrote a prescription for 120 oxycodone pills in exchange for $150 in cash. *Id.* ¶ 25. After the initial meeting, at Dr. Mayard's instruction, that same patient provided the doctor with lists of names of his "family or friends," and Dr. Mayard sold him prescriptions written in those names for $200-$300 each. *Id.*

A review of records revealed that from approximately 2009 through 2012, Dr. Mayard issued approximately 6,500 oxycodone prescriptions authorizing the dispensing of more than 700,000 pills. *Id.* ¶ 24. On March 13, 2013, more than a month after Dr. Mayard surrendered his DEA registration, a pharmacy in Suffolk County, New York alerted the DEA that a customer had presented a prescription for oxycodone signed by Dr. Mayard. *Id.* ¶¶ 26-29. Dr. Mayard confirmed by telephone that he had written the prescription. *Id.* ¶ 29. When confronted with the fact that he could not legally issue the prescription without a current DEA registration, Dr. Mayard advised the pharmacist to "give it back to the patient and I'll work it out with her." *Id.*

Based on this information, the undersigned issued the warrant for Dr. Mayard's arrest.

The Application for Geolocation Data

On March 19, 2013, as part of its efforts to execute the arrest warrant, the Government made two contemporaneous applications regarding a cell phone used by Mayard. First, an Assistant U.S. Attorney, certifying that the information requested likely would be relevant to "an ongoing criminal investigation to apprehend [Dr.] Mayard," sought an order authorizing the use of a pen register and trap and trace device under 18 U.S.C. §§ 3122 and 3123 in connection with the subject telephone. Second, the Government moved under Federal Rule of Criminal Procedure 41(c) and 18 U.S.C. § 2703(c)(1)(A) for authorization to obtain location data – specifically prospective cell-site data – concerning the same mobile telephone.

In support of the application for geolocation data, a DEA Task Force officer averred that efforts had been made to arrest Dr. Mayard at several locations, including his known residences and offices. Affidavit in Support of Application for a Search Warrant ¶ 5, DE [1] ("Search Affidavit"). Having failed to apprehend Dr. Mayard, officers called him at the subject telephone. *Id.* Dr. Mayard spoke with the officers who attempted to convince him to surrender. Dr. Mayard both refused to surrender or provide any information about his location. *Id.* Based on these facts, the Government contended that there was probable cause to believe that Dr. Mayard was using the subject telephone as part of an effort to flee from justice.[1] *Id.* ¶ 3. As part of this application, the Government sought not only prospective geolocation data for a period of up to 30 days, but additionally requested an order directing the relevant telecommunications carrier to "initiate a signal to determine the location of the subject telephone" and that such signal be sent "unobtrusively." *Id.* ¶ 8.

[1] The Government expressly reserved its right to argue that it could obtain prospective cell-site information without showing probable cause under the authority of 18 U.S.C. § 2703(d). Search Aff. ¶ 3 n.1.

Because of the exigency of the situation, the undersigned granted both applications, issuing a short form order indicating a full opinion would follow. Order That There is Probable Cause, Mar. 19, 2013, DE [6].

The Arrest

The following day, using geolocation data garnered as a result of the authorization order, agents located Dr. Mayard in a car on a street in Queens. Application for Search Warrant ¶ 5, *United States v. Items Contained Within One Black Nylon Swiss Gear Bag*, No. 13-MJ-262 (E.D.N.Y. Mar. 22, 2013) ("Hill Affidavit"). That car was owned by an individual for whom the defendant had prescribed controlled substances in the past, and who was present at the time of his arrest. *Id.* ¶ 5; Arraignment Hr'g Tr. 12:16-23, DE [8] *United States v. Mayard*, No. 13-MJ-238 (E.D.N.Y. Mar. 20, 2013) ("Bail Hearing"). Mayard was found in possession of the subject cellular phone – a Blackberry Curve Model number 9360 – as well as two additional smartphones and an iPad mini. Tellingly, Dr. Mayard's car contained a number of items suggestive of flight – luggage, clothing, grocery bags containing food and a cooler. Hill Aff. ¶ 5. Dr. Mayard had in excess of $7,000 in cash and an expired passport on his person. *Id.* Tucked inside the passport, agents found a pair of passport-sized photographs depicting Dr. Mayard in the same clothing he wore at the time of his arrest. *Id.* That passport also contained a scrap of paper bearing the instruction to email an itinerary to a particular email address at the U.S. Department of State, which, according to Government counsel, constitutes part of the procedure for obtaining an expedited passport. Bail Hr'g Tr. 14:22-15:5. Inside his vehicle, agents also discovered shredded prescription forms. Hill Aff. ¶ 7.

Following a hearing, Dr. Mayard was held without bail pursuant to a permanent order of detention, predicated primarily on risk of flight and the danger to the community. Order of Detention, DE [6], *United States v. Mayard*, No. 13-MJ-238 (E.D.N.Y. Mar. 20, 2013).

DISCUSSION

Search Warrants to Aid in Apprehension of a Defendant

In its application, the Government demonstrated that agents were attempting to apprehend Dr. Mayard based upon the March 18 arrest warrant, that he was aware of the charges and had declined repeated invitations to surrender.[2] Furthermore, the Government demonstrated that the data sought – prospective cell-site information about defendant's cell phone – could reasonably assist in his apprehension because, among other things, agents had been able to twice contact him on that cell phone within a day of the application. The question then is whether such a showing is sufficient to sustain a search warrant for information that reasonably could facilitate capture of the defendant. That question should be readily answered in the affirmative.

Surprisingly, however, a fairly recent decision concludes the opposite. In *In re Application*, 849 F. Supp. 2d 526 (D. Md. 2011), a magistrate judge denied the Government's application for geolocation data, holding that a federal court may not issue a search warrant "to aid in the apprehension of the subject of an arrest warrant" in the absence of a showing of additional criminal activity. *Id.* at 530.

In reaching this conclusion, *In re Application* rejects a long line of Supreme Court cases advising that "it is reasonable, within the terms of the Fourth Amendment, to conduct otherwise permissible searches for the purpose of obtaining evidence which would aid in apprehending and convicting criminals." *Warden v. Hayden*, 387 U.S. 294, 306-307, 87 S. Ct. 1642, 1650 (1967). The Supreme Court explained that "probable cause must be examined in terms of cause to

[2] Though unnecessary for this determination, these facts render the defendant a fugitive under applicable law. *See United States v. All Funds on Deposit*, 801 F. Supp. 984, 998 (E.D.N.Y. 1992) (individual deemed a fugitive upon demonstration that "the person sought in the criminal proceeding knows he is wanted by the authorities and then fails to submit to arrest").

believe that the evidence sought will aid in a particular apprehension or conviction."[3] *Id.* And while *In re Application* dismisses this language as "*dicta* - intriguing *dicta* - but *dicta*," *In re Application* at 561, the Supreme Court has consistently reiterated this formulation. *Messerschmidt v. Millender*, 132 S. Ct. 1235, 1248 (2012) ("The Fourth Amendment require[s] only 'probable cause ... to believe the evidence sought *will aid* in a particular apprehension or conviction'") (emphasis in the original); *Dalia v. United States*, 441 U.S. 238, 255, 99 S. Ct. 1682, 1692 (1979) (same); *Andresen v. Maryland*, 427 U.S. 463, 483, 96 S. Ct. 2737, 2749 (1976) ("probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction"); *Zurcher v. Stanford Daily*, 436 U.S. 547, 583, 98 S. Ct. 1970, 1990 (1978) (Stephens, J. dissenting) (same).

The Second Circuit has quoted the *Warden v. Hayden* "aid in apprehension" language in several opinions. *Hines v. Albany Police Dept.*, Nos. 11–CV–2947 and 12–CV–1126, 2013 WL 1276559, at *1 (2d Cir. Mar. 29, 2013) (upholding determination of that vehicle was seized unlawfully where "there is nothing in the record to suggest that the vehicle was or contained evidence—that is, material that would 'aid in a particular apprehension or conviction'"); *United States v. Ochs*, 595 F.2d 1247, 1258 (2d Cir. 1979) ("probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction"); *United States v. Bennett*, 409 F.2d 888, 897 (2d Cir. 1969). Nearly every other circuit has similarly quoted this language with approval. *See, e.g.*, *United States v. Hager*, 710 F.3d 830, 836 (8th Cir. 2013) (determining whether evidence sought would "aid in a particular apprehension or conviction."); *United States v. Christine*, 687 F.2d 749, 760 (3d Cir. 1982)

[3] While the Government did not invoke this argument here, evidence of the locus or movements of a defendant being sought may not only assist in the apprehension of that defendant, but may well facilitate conviction as well. It has long been established that "the law is entirely well settled that the flight of the accused is competent evidence against him as having a tendency to establish his guilt." *Allen v. United States*, 164 U.S. 492, 499, 17 S. Ct. 154, 157 (1896).

(same); *United States v. Anton*, 633 F.2d 1252, 1254 (7th Cir. 1980) ("Probable cause exists when it is reasonably believed that the evidence sought will aid in a particular apprehension or conviction"). Given this uninterrupted line of authority, this Court will not reject as mere surplusage the Supreme Court's consistent statement that a federal court may issue a search warrant, based on probable cause, to assist in the apprehension of a fugitive. *But see In Re Application* at 536 ("current Fourth Amendment jurisprudence [does not] authorize[] use of a search warrant to obtain information to aid in the apprehension of the subject of an arrest warrant where there is no evidence of flight to avoid prosecution and the requested information does not otherwise constitute evidence of a crime").

Numerous cases contemplate the issuance of search warrants to assist officers seeking to make an arrest. Most notably, in *Steagald v. United States*, 451 U.S. 204 (1981), the Supreme Court considered the extent to which an arrest warrant authorized an officer to search private homes for a fugitive, ultimately concluding that entry into a home other than the residence of the fugitive required the issuance of a search warrant. The Court held:

> Because [an arrest warrant] does not authorize the police to deprive the third person of his liberty, it cannot embody any derivative authority to deprive this person of his interest in the privacy of his home. Such a deprivation must instead be based on an independent showing that a legitimate object of a search is located in the third party's home. We have consistently held, however, that such a determination is the province of the magistrate, and not that of the police officer.

Id. at 214. Thus, under certain circumstances, the express holding of *Steagald* requires the Government to seek search warrants in aid of the execution of an arrest warrant to make an apprehension.

In Re Application, though, attempts to distinguish the issuance of a warrant to search for a defendant in a particular place from a search warrant for information that could lead to the

defendant's capture. *In Re Application* at 563. As to the latter category, *In Re Application*, noting the scant case law dealing with such searches, concludes that "a warrant [for information leading to an apprehension] is unavailable where there is no evidence of flight." *Id.* at 562-64. There are not many reported cases concerning a search warrant for data leading to the location of a wanted defendant, as this particular situation does not arise frequently in situations that encourage review. However, in *United States v. Ellis*, 461 F.2d 962 (2d Cir. 1972), the Second Circuit upheld the warrantless search of an automobile where an officer "thought that the automobile contained evidence which might aid in the apprehension of the two criminals still at large and that waiting for a warrant might enable them to evade capture." *Id*. at 966. Similarly, *United States v. Robinson*, 533 F.2d 578, 583 (D.C. Cir. 1975), upheld the warrantless search of an automobile that "could well produce the information needed to speedily apprehend the culprits," noting that "delay to obtain a warrant would have impeded a promising police investigation and conceivably provided the added time needed by the bank robbers to avoid capture altogether." Clearly, the decisions in *Ellis* and *Robinson* envisage the issuance of a search warrant to seek information of the location of wanted individuals who remain at large.

In providing "guidance" to the Government, *In re Application* suggests that an application for prospective geolocation data:

> requires a showing of probable cause that: 1) a valid arrest warrant has issued for the user of the subject cellular telephone; 2) the subject cellular telephone is in the possession of the subject of the arrest warrant; and 3) the subject of the arrest warrant is a fugitive, that is, is or could be charged with violation of 18 U.S.C. § 1073.

Id. at 537. Specifically, *In re Application* provides that, before a search warrant may issue, "the government must demonstrate that the defendant fled the state with the intent of avoiding prosecution." *Id*. at 567. Holding the government to this level of proof at the search warrant stage does not comport with existing law. As the Supreme Court has noted:

> Chief Justice Marshall observed . . . that "the term 'probable cause,' according to its usual acceptation, means less than evidence which would justify condemnation . . . . It imports a seizure made under circumstances which warrant suspicion." More recently, we said that "the *quanta* ... of proof" appropriate in ordinary judicial proceedings are inapplicable to the decision to issue a warrant. Finely-tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision. While an effort to fix some general, numerically precise degree of certainty corresponding to "probable cause" may not be helpful, it is clear that "only the probability, and not a prima facie showing, of criminal activity is the standard of probable cause."
>
> We also have recognized that affidavits are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleading have no proper place in this area. Likewise, search and arrest warrants long have been issued by persons who are neither lawyers nor judges, and who certainly do not remain abreast of each judicial refinement of the nature of "probable cause." … [M]any warrants are -- quite properly -- issued on the basis of nontechnical, common-sense judgments of laymen applying a standard less demanding than those used in more formal legal proceedings.

Illinois v. Gates, 462 U.S. 213, 235-236, 103 S. Ct. 2317, 2330-2331 (1983) (internal citations and quotation marks omitted). Demanding that the Government demonstrate each element of § 1073 before granting a search warrant to assist in the apprehension of a defendant is inconsistent with these standards and common sense.

Because the apprehension of fugitives is an important societal objective, the law authorizes the issuance of search warrants for significant invasions of privacy – such as the search of a home of a third-party – to locate a defendant sought pursuant to an arrest warrant. Clearly, then, the Court is authorized to issue a search warrant for the far less intrusive search sought here – obtaining data reflecting the location of defendant's cell phone. *United States v. Bermudez*, No. IP 05-43-CR-B/F, 2006 WL 3197181, at *11 (S.D. Ind. June 30, 2006) (arrest warrant "gave law enforcement the authority to physically enter a target's home in order to search for the target; and also gave law enforcement the authority to conduct a less intrusive search for the fugitive by tracking cell location information in an effort to locate him").

The facts and circumstances of this case – including events that occurred after issuance of the geolocation authorization – help demonstrate the critical need for such targeted information. The defendant appears to have engaged – brazenly – in dangerous, criminal conduct over an extended period, undeterred by efforts to curtail these activities, including the specter of a DEA investigation and surrender of his controlled substances registration. Perhaps unsurprisingly, defendant refused to surrender or provide information about his whereabouts after being advised of this Court's issuance of an arrest warrant. The articles found in his possession, including evidence of his efforts to obtain an expedited passport, and the food, clothing and cash found in an automobile titled to a criminal co-conspirator, suggest that the defendant intended to flee the country to avoid facing the pending charges. Without the use of the subject geolocation data to find the defendant, he might well have succeeded, frustrating efforts to resolve the pending charges and the proper administration of justice.

Thus, I find that where, as here, the Government demonstrates probable cause to believe that prospective geolocation data will aid in the apprehension of a defendant, a court may issue a search warrant to authorize access to such data.

There is no Reasonable Expectation of Privacy in Prospective Cell-Site Data

Geolocation Technology and the Rise of the Smartphone

Like many aspects of technology, geolocation has advanced at a bewildering pace, and courts and lawmakers have struggled to adapt the law to these innovations. A brief look at the improvements in geolocation technology and the public awareness of those developments provides important context.

The advent of the smartphone has dramatically changed the ways in which we use and understand cellular telephone devices. Manufacturers modeled early cell phones on traditional landline telephones, to wit: a device used to communicate via audio conversation. Smartphones

represent an entirely different paradigm. Contemporary smartphones, which continue to evolve,[4] are equipped with a panoply of technologies, allowing users not only the ability to make and receive audio calls, but also access to the Internet, text messages, video calls, email and thousands of software applications. Many of these features are akin to those formerly associated with a personal computer.

One important aspect of smartphone technology is the ability of these devices to identify, in real time, their geographic location, which data can be shared with certain programs and providers to enable advanced functions. At present, three techniques are used to generate this information. The collection of cell-site data – the identification of the radio cell tower or towers nearest to the device – is the oldest geolocation technology and the one at issue in this case. Cell-site location is arguably the least precise of the three methods currently used, though that precision can be substantially enhanced through triangulation of signals from multiple towers. Global Positioning System (GPS) data is a technique by which radio signals are received by the smartphone from a system of satellites in geosynchronous orbit and interpreted by programs to provide highly accurate location data. Wireless geolocation operates by comparing the access points used by the smartphone to connect to the Internet against a database of known router locations. Depending on the quality of the information in the database, this method, though similar to cell-site location, can be far more accurate because wireless transmissions have a shorter range than cellular transmissions. Additional emerging geolocation technologies,

[4] The Oxford English Dictionary captures the evolutionary nature of smartphones in its definition of the term: "Originally: any of various telephones enhanced with computer technology. Later chiefly: *spec.* a mobile phone capable of running general-purpose computer applications, now typically with a touch-screen interface and Internet access." *See* Oxford English Dictionary, "smartphone," http://www.oed.com/view/Entry/381083.

including Bluetooth beacons, reportedly have the potential to pinpoint the location of a phone to a matter of inches.[5]

Taken together, these innovations enable smartphones and associated apps to provide a broad range of functions, from the vital to the prosaic. Enhanced 9-1-1 systems transmit geolocation data to 9-1-1 dispatchers, allowing police and first responders to pinpoint callers in emergency situations.[6] Map programs employ location data to provide smartphone users with turn-by-turn driving directions. Geolocation data offers access to localized weather information, and "find my phone" apps permit users to recover lost or stolen smartphones. Parents use location functions to keep tabs on their children.[7] Advertisers obtain access to geolocation data to promote nearby businesses.

Smartphones contain settings that allow users to disable the geolocation functions of their smartphones generally or specifically limit the data provided to a particular application.[8] For example, the User Guide for the Blackberry Curve 9360 – the smartphone used by the defendant in this case – provides instructions for deactivating geolocation services, warning users that "[i]f you turn on geolocation in the browser, some websites might be able to determine your

---

[5] *See generally* Stephen Lawson, *Ten Ways Your Smartphone Knows Where You Are*, PCWorld, April 6, 2012, http://www.pcworld.com/article/253354/ten_ways_your_smartphone_knows_where_you_are.html.

[6] *See* Federal Communications Commission, Enhanced 9-1-1 - Wireless Services, http://transition.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html.

[7] In a recent study of mobile smartphone apps aimed at children, the Federal Trade Commission found that at least 3% of the applications studied – some of which had been downloaded several hundred thousand times – collected geolocation data and other identifiers from smartphones, which was often transmitted to advertising networks. Federal Trade Commission, Mobile Apps for Kids: Disclosures Still Not making the Grade 10-11 (2012), *available at* http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.

[8] The Apple iPhone User Agreement provides that "**By using any location-based services on your iOS Device, you agree and consent to Apple's and its partners', licensees' and third party developers' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** You may withdraw this consent at any time by going to the Location Services setting on your iOS Device and either turning off the global Location Services setting or turning off the individual location settings of each location-aware item on your iOS Device. Disabling these location features will only impact the location-based functionality of your iOS Device." Apple Inc. iOS Software License Agreement ¶ 4(b), http://www.apple.com/legal/sla/docs/ios6.pdf (emphasis in original).

approximate location."[9] Turning off these settings interferes with the proper functioning of applications dependent on geolocation data: a user in New York may find that the map program displays maps of Washington, D.C., or may only be able to retrieve weather information for Cupertino, California. Apps that rely on geolocation technology generally prompt the user for "permission" to access location information and, if permission is refused or geolocation is turned off, will regularly alert the user to reactivate the settings. Thus, smartphone users become well aware of these settings based on these frequent notifications and reminders.

Importantly, turning off the power on any smartphone or cell phone disables all geolocation technologies. A cellular telephone that is not powered on – or one that has a drained battery – simply cannot be located. This fact is widely known and readily accessible. As one non-technical website advises:

> Turn off your cell phone. It's as easy as that. If your cell phone is turned off, it's not transmitting signals that can be picked up by cell towers, and if it has a built-in GPS device, it can't be tracked.[10]

An Internet search on the question of preventing cell phone tracking turns up scores of sites offering the very same advice.

The newsworthiness of cell phone tracking as a concept has waned, confirming that geolocation has moved from the unfamiliar to the commonplace. More than a dozen years ago, the *New York Times* reported on the Enhanced 9-1-1 effort, predicting that "by next year cell phones sold in the United States will be equipped with advanced wireless tracking technology," and raising privacy concerns connected with the ability to pinpoint the location of a particular

[9] User Guide, Blackberry Curve Series, *available at* http://docs.blackberry.com/en/smartphone_users/deliverables/38073/BlackBerry_Curve_Series-User_Guide--1817681-0105044128-001-7.1-US.pdf.

[10] eHow.com, *How to Prevent Cell Phone Detection*, http://www.ehow.com/how_5974027_prevent-cell-phone-detection.html (last visited Apr. 23, 2013).

phone.[11] By 2005, the same news outlet observed that "[m]ost Americans carry cellphones, but many may not know that government agencies can track their movements through the signals emanating from the handset."[12] Last year, the *Times* dubbed such efforts by police as "a routine tool," observing that "the wide use of cell surveillance has seeped down to even small, rural police departments."[13] In a feature story about the defendant's arrest in this very case, *Newsday*, a top-ten media outlet with nearly 400,000 subscribers,[14] devoted only eight words to the fact that Dr. Mayard "was tracked down in Queens through his cellphone."[15]

Though awareness of geolocation itself has become pervasive, specific manifestations of this technology continue to capture public attention, including the following:

- **Footpath Technology –** A British IT company developed Footpath Technology, which "consists of antennas placed around the mall that capture a phone's unique identification system (similar to an IP address), and tracks where the phone goes around the mall."[16] Essentially, this system mimics cell tower triangulation on a micro scale, with far greater precision, allowing merchants to track the movements of shoppers about the mall. Several U.S. retailers planned to deploy Footpath for the 2011 holiday shopping season until Senator Charles Schumer intervened, demanding review by the Federal Trade Commission. Senator Schumer issued press releases, widely disseminated in the media, advising the public, "If a shopper does not want to be tracked, their only option is to turn off their cell phone."[17] The Senator's actions dissuaded retailers from their initial deployment of the technology, and drew considerable attention to the issue.[18]

---

[11] Simon Romero, *Location Devices' Use Rises, Prompting Privacy Concerns*, N.Y. Times, Mar. 4, 2001, http://www.nytimes.com/2001/03/04/business/location-devices-use-rises-prompting-privacy-concerns.html?pagewanted=all&src=pm.

[12] Matt Richtel, *Live Tracking of Mobile Phones Prompts Court Fights on Privacy*, N.Y. Times, Dec. 10, 2005, http://www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=all.

[13] Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. Times, Mar. 31, 2012, http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?pagewanted=all.

[14] *See* Alliance for Audited Media, *Top 25 U.S. Newspapers for September 2012*, http://www.auditedmedia.com/news/research-and-data/top-25-us-newspapers-for-september-2012.aspx (last visited Apr. 29, 2013).

[15] Ellen Yan and Robert Kessler, *Gracia Mayard, Queens doctor charged in illegal oxycodone distribution, captured*, Newsday, Mar. 20, 2013, http://www.newsday.com/long-island/gracia-mayard-queens-doctor-charged-in-illegal-oxycodone-distribution-captured-1.4849466.

[16] Sean Kane, *This Holiday Season, Your Mall May be Tracking Your Behavior*, Popular Science, Nov. 23, 2011, http://www.popsci.com/technology/article/2011-11/your-mall-might-be-watching-you-holiday-season.

[17] *See* Press Release, Senator Charles E. Schumer, Schumer Reveals: This Holiday Season, New Technology Could Be Tracking Shoppers' Movements In Shopping Centers Through Their Cell Phones; Calls For Mandatory Opt-In Before Retailers Are Allowed To Track Shoppers' Movements (Nov. 28, 2011), *available at* http://www.schumer.senate.gov/Newsroom/record.cfm?id=334975.

[18] "Tracking test halted on privacy worries," Boston Globe, Nov. 29, 2011, http://www.boston.com/business/technology/articles/2011/11/29/tracking_test_halted_on_privacy_worries/.

- **Find My Phone –** In the summer of 2012, David Pogue, technology correspondent for the *New York Times*, lost his iPhone on a train ride from Philadelphia to Connecticut. Pogue triggered the "Find My Phone" service, which employs geolocation technology to help users recover lost or stolen cell phones. Pogue soon learned that his phone was in or near a home in Seat Pleasant, Maryland, information that he shared with 1.4 million readers via Twitter. GPS readings suggested that the phone travelled in and out of the home, though these shifts may have been attributable to imprecision in the location technology. Recovering Pogue's iPhone became a cause célèbre, with the writer and his readers posting maps and photos of the home. The police conducted a search and recovered the iPhone from the backyard of the home, returning it to its owner.[19] Reportedly, the homeowner was implicated in the theft of the device, but Pogue declined to press charges.[20] Media outlets across the country carried the story, some focusing on the privacy implications of the technology. Confronted with that issue, Pogue noted that "cell phone companies do know where you are at all times. They have triangulation at any time. So, if you don't want cell phones not to have the potential of knowing where you are, don't own a cell phone."[21]

- **Girls Around Me: the "Stalker App"** – The Girls Around Me app, which surfaced in March 2012, represents a highly disturbing manifestation of geolocation technology. The program drew data from the web service "Foursquare," through which users got "virtual rewards" (such as online badges) for checking in at various public establishments identified via their smartphone's GPS location software. Their location, in turn, would be broadcast to other users in an effort to both promote these establishments and create opportunities for social interaction. The Girls Around Me app correlated this geolocation data with personal identifiers publicly available on Facebook to perform an unusual function: by clicking on the Girls Around Me icon (a James Bond film-like silhouette against the backdrop of a radar screen), the user was presented with a map showing photographs and personal details of young women located nearby, including their names, ages, marital status, dates of birth and interests.[22] After a prominent blogger wrote about the Girls Around Me app, it made national news, and the growing infamy led to its withdrawal. Yet, as the developers of the app noted in a defense of their efforts, the app did nothing more than aggregate (though in a highly distasteful manner) geolocation and personal information already available to the public.[23]

Cognizance of geolocation apps and their implications has become so widespread that, according to a recent study, "[n]early 60% of smartphone users employ apps that access their location data

---

[19] *See generally* David Pogue, *Where is David Pogue's iPhone?*, N.Y. Times, Aug. 2, 2012, http://pogue.blogs.nytimes.com/2012/08/02.
[20] *Privacy in a Digital Age: When Twitter Followers Can Track a Lost Phone*, PBS Newshour, Aug. 3, 2012, http://www.pbs.org/newshour/bb/media/july-dec12/phone_08-03.html.
[21] *Id.*
[22] *See* John Brownlee, *This Creepy App Isn't Just Stalking Women Without Their Knowledge, It's A Wake-Up Call About Facebook Privacy*, Cult of Mac, Mar. 30, 2012, http://www.cultofmac.com/157641.
[23] *See, e.g.*, Julia Angwin, *What They Know, A Wall Street Journal Investigation: The Selling of You*, Wall St. J., Apr. 7, 2012.

despite having concerns about risks to their privacy and even personal safety."[24] As an attorney for the ACLU observed last year, "While law enforcement sometimes argues that making members of the public aware that cell phone companies can track them will make it more difficult to catch criminals, it is too late in the day for that argument now that cell phone tracking is a staple of television police procedurals."[25]

Finally, due to business practices in the IT industry, cell phone users like the defendant not only are made aware that their cell phone may be tracked and this information may be provided to authorities, but they expressly agree to these terms before operating the cell phone.[26] For example, T-Mobile, the carrier in this case, requires users to agree to terms and conditions that include its privacy policy, which governs company's use of personal information.[27] That policy provides that:

- T-Mobile may automatically collect your information when you use your mobile device or T-Mobile services or websites, including:
  - Your phone number and device identifier [and]
  - The location of your device on our network and the GPS location of your device …

- … We will provide customer information where necessary to comply with the law, such as disclosure of your information to a law enforcement agency for your safety or the safety of others, or when compelled by subpoena or other legal process.[28]

[24] Cameron Scott, *Geolocation apps draw users, despite privacy concerns*, Computerworld, Apr. 3, 2012, http://www.computerworld.com/s/article/9225820.
[25] Catherine Crump, *Are the police tracking your calls?*, CNN, May 21, 2012, http://www.cnn.com/2012/05/22/opinion/crump-cellphone-privacy.
[26] In fact, geography plays a critical part in the selection of a telecommunications carrier. "Before choosing a wireless service provider or a plan, it is wise to research the various providers to determine the extent of their coverage in the areas that matter most to you." Federal Communications Commission, Understanding Wireless Telephone Coverage Areas 1, *available at* http://transition.fcc.gov/cgb/consumerfacts/cellcoverage.pdf.
[27] *See* T-Mobile Terms & Conditions (effective December 30, 2011), *available at* www.t-mobile.com/Templates/Popup.aspx?PAsset=Ftr_Ftr_TermsAndConditions&print=true ("Our Privacy Policy governs how we collect and use information related to your use of our Service and is available online . . .").
[28] T-Mobile Privacy Policy, *available at* https://www.t-mobile.com/company/website/privacypolicy.aspx.

Other carriers and smartphone manufacturers maintain comparable privacy policies incorporated into terms and conditions of service.[29] Here, Research in Motion, maker of the Blackberry smartphone at issue, provides in its privacy policy that:

> When you use RIM Offerings, enable data services, use the browser or location-based functionality on your device, location information associated to your device (e.g. Global Positioning System (GPS) or similar satellite triangulation information, carrier or tower ID, the BSSID (Broadcast Service Set Identifier) and MAC address (Media Access Control address) of Wi-Fi access points, and signal strength of visible Wi-Fi hotspots or wireless towers) may be communicated to RIM or our service providers. . . . RIM may process such information to provide you with or facilitate the provision of information and location-based services (e.g. mapping services, measuring traffic congestion, location-sensitive promotions or coupons). If you choose to use location-based services, you agree that such geographic location information may be processed to provide you with such services. You may manage through the settings on your device either the overall settings for your device's GPS or location functionality or individual settings for each application. . . .
>
> In certain circumstances, your personal information may be processed without your consent depending on the jurisdiction and any applicable laws. For example, RIM may not seek consent . . . to comply with a subpoena, warrant or other court order, lawful request or legal process; or as may be otherwise required or permitted by law.[30]

Thus, based on industry practice, cell phone users agree, both with their telecommunication carrier and the smartphone manufacturer, that their geolocation information may be tracked and provided, without notice or consent, to authorities or other third parties based upon a subpoena or court order.

Inapplicability of the Fourth Amendment to Geolocation Data

The Fourth Amendment of the United States Constitution provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants

[29] *See ,e.g.*, Verizon Privacy Policy, *available at* www22.verizon.com/about/privacy/policy/ (providing that Verizon may disclose customer identification information "to comply with valid legal process including subpoenas, court orders or search warrants").

[30] Research in Motion, Privacy Policy (Aug. 2012), *available at* http://us.blackberry.com/legal/privacy-policy.html; *cf.* Research in Motion, Terms and Conditions of Use, *available at* us.blackberry.com/legal/terms-and-conditions.html.

> shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

US Const. amend. IV. Recently, the Supreme Court grappled with the application of the Fourth Amendment to one form of electronic location monitoring, to wit: the warrantless installation and monitoring of a GPS tracking device on a defendant's automobile where "the Government trespassorily inserted the information-gathering device." *United States v. Jones*, 132 S. Ct. 945, 952 (2012). In concluding that the evidence obtained violated the defendant's rights under the Fourth Amendment, the Court relied upon principles of common-law trespass, noting that these principles were closely linked to Fourth Amendment jurisprudence "at least until the latter half of the 20th century." *Id.* at 949. While drawing on these principles, the Court cautioned:

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.

Id. at 949. The Court clearly distinguished that case from "situations involving merely the transmission of electronic signals without trespass [that] would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original). Therefore, procuring prospective cell site data, which involves only the transmission of electronic signals without trespass, would be subject to the standard set out in *Katz v. United States*, 389 U.S. 347, 351, 88 S. Ct. 507, 19 L.Ed.2d 576 (1967) (suppressing conversation intercepted from recording defendant with device planted in public telephone booth).

The *Katz* analysis, of course, refers to the now-familiar formulation contained in Justice Harlan's concurrence, which requires:

> [F]irst, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of

> outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable. The critical fact in this case is that '(o)ne who occupies it, (a telephone booth) shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted.

Katz, 389 U.S. at 361 (citation omitted).

The Second Circuit has not ruled directly on the question of whether a user has a reasonable expectation of privacy in geolocation data, though it has supplied some guidance on the question. In *United States v. Pascual*, No. 11-CR-2988, 2012 WL 5476657 (2d Cir. Nov. 13, 2012), the defendant argued that "the district court improperly admitted cell-site records secured pursuant to a subpoena, without a warrant or a showing of probable cause." *Id.* at *4. Because the defendant failed to preserve the issue, it was reviewed for plain error. The Circuit observed that the defendant's position was "(at the very least) in some tension with prevailing case law," citing *Smith v. Maryland*, 442 U.S. 735, 742–44, 99 S. Ct. 2577, 61 L.Ed.2d 220 (1979) (a customer has no reasonable expectation of privacy in dialed phone number conveyed to telephone company), and *United States v. Miller*, 425 U.S. 435, 443, 96 S. Ct. 1619, 48 L.Ed.2d 71 (1976) (Fourth Amendment inapplicable to information conveyed to a third party). *Pascual* concluded that it "was not plain error for the district court not to anticipate this innovative argument and *sua sponte* exclude the evidence, when no governing precedent from this Court or the Supreme Court required exclusion, and the general principles adopted by those courts pointed the other way." *Id.*

In *United States v. Skinner*, the Sixth Circuit considered the issue directly, as the defendant claimed that "the use of the GPS location information emitted from his cell phone was a warrantless search that violated the Fourth Amendment." *United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012). *Skinner* holds that

> There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone. If a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal.

Id.; *cf. In re Applications of the United States for Orders Pursuant to Title 18, U.S. Code Section 2703(d)*, 509 F. Supp. 2d 76, 81 (D. Mass. 2007) (no Fourth Amendment interest in prospective cell-site data).

In large part, the Sixth Circuit relied upon the fact that "Skinner was traveling on a public road before he stopped at a public rest stop. While the cell site information aided the police in determining Skinner's location, that same information could have been obtained through visual surveillance." *Skinner*, 690 F.3d at 778. Other cases in this area similarly rely on the defendant's presence in a public area as a basis to determine that no Fourth Amendment issue exists. *See, e.g., United States v. Knotts*, 460 U.S. 276, 281 (1983) ("The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways. . . . A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). While helpful deciding suppression motions, such *ex post* analyses may not provide a useful framework for issuing authorization to obtain cell site data, as at the time of application it generally remains unknown whether the data sought may reveal movements in non-public spaces.

Other decisions have relied on the limitations of the technology to ensure a measure of privacy. However, as smartphones utilize multiple, ever-improving technologies, this factor remains elusive, and thus an unreliable foundation upon which to construct constitutional doctrine. *Cf. In re Application of the United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F.Supp.2d 202, 208 (E.D.N.Y. 2008) ("The specter of

such precise location tracking does not loom over this case, because the Government is seeking only information identifying the one antenna tower . . . . Such information, unlike the information revealed by triangulation or by more advanced communications devices like the iPhone, which contain Global Positioning System devices, is not precise enough to enable tracking of a telephone's movements within a home.").

In the context of historical cell site information, some judges have considered the length of the proposed monitoring – approving shorter, discrete periods while rejecting applications for data covering extended periods. *See, e.g.*, *In re Application of the United States for an Order Authorizing Release of Historical Cell-Site Information*, No. 11-MC-113, 2011 WL 679925, at *1 (E.D.N.Y. Feb. 16, 2011) ("the shorter time period of the surveillance at issue here distinguishes the instant application from the ones that I have denied on constitutional grounds"). However, in *Jones*, the Court rejected this approach as "a novelty" that "remains unexplained." *Jones*, 132 S. Ct. at 954; *see also United States v. Jones*, --- F. Supp. 2d ---, No. 05-0386, 2012 WL 6443136, at *6 (D.D.C. Dec. 14, 2012). Further, the temporal length of the request is more relevant to requests for historical geolocation data than to the prospective acquisition of geolocation data. For example, in this case, the undersigned granted authorization for a thirty day period, but the Government obtained the information required in one day.

In light of the development and general awareness of geolocation technologies, I believe that the voluntary disclosure doctrine provides the most important departure point in evaluating requests for prospective data. The Supreme Court has held that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *United States v. Miller*, 425 U.S. at 443. In *Smith v. Maryland*, 442 U.S. at 743-4, the Supreme

Court applied the principal that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" specifically in the context of telecommunications data.

The *Smith* Court held that a pen register – a device that records telephone numbers dialed by a subscriber – was not subject to the Fourth Amendment's warrant requirement, finding that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the contents of communications." *Id.* at 741. The Court thus drew on a critical distinction in the area of communications – the difference between content and non-content information. This distinction is deeply rooted in our jurisprudence: higher protection is afforded to information contained within a communication than to information incidental to that communication. *See Ex parte Jackson*, 96 U.S. 727, 733, 24 L. Ed. 877 (1877) ("[l]etters and sealed packages . . . are as fully guarded from examination and inspection, except as to their outward form and weight"). Like dialed telephone numbers, geolocation data falls squarely into non-content information, as distinct from the contents of calls, texts and emails that can be sent to and from a smartphone.

The Court in *Smith* then analyzed the expectation of privacy in pen register data:

> Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.
>
> This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. . . . Telephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

442 U.S. at 741-44. Cell phone customers similarly convey geolocation data to their telephone carriers, and cannot possibly labor under the belief that their location is somehow kept secret from telecommunication carriers and other third parties. Under existing law, then, a user does not have a reasonable expectation of privacy as to geolocation data.

At least one court, however, has attempted to distinguish *Smith* from prospective cell phone data, finding:

> Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge.

In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F.Supp.2d 747, 756-57 (S.D. Tex. 2005). I cannot agree. As demonstrated above, it is clearly within the knowledge of cell phone users that their telecommunication carrier, smartphone manufacturer and others are aware of the location of their cell phone at any given time. *See In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F.Supp.2d 113, 121 (E.D.N.Y. 2011) ("Public ignorance as to the existence of cell-site-location records . . . cannot long be maintained"). After all, if the phone company could not locate a particular cell phone, there would be no means to route a call to that device, and the phone simply would not work. Given the notoriety surrounding the disclosure of geolocation data to retailers purveying soap powder and blue jeans to mall shoppers, the police searching for David Pogue's iPhone and, most alarmingly, the creators and users of the Girls Around You app, cell phone users cannot realistically entertain the notion that such information would (or should) be withheld from federal law enforcement agents searching for a fugitive.

As to control by the user, all of the known tracking technologies may be defeated by merely turning off the phone. Indeed – excluding apathy or inattention – the only reason that

users leave cell phones turned on is so that the device can be located to receive calls. Conversely, individuals who do not want to be disturbed by unwanted telephone calls at a particular time or place simply turn their phones off, knowing that they cannot be located.

A central element in determining whether an individual has a reasonable expectation of privacy is the effort made to keep the subject information private. Justice Harlan noted that it was a "critical fact" that Katz "shut[] the door behind him" when entering the phone booth in determining that he had a reasonable expectation of privacy. Even where a defendant has made Herculean efforts to protect privacy, he may still not have a reasonable expectation of privacy. In *California v. Ciraolo*, 476 U.S. 207, 209, 106 S. Ct. 1809, 1810, 90 L. Ed. 2d 210 (1986), the Court reviewed claims of Fourth Amendment violations by a defendant who erected a "6-foot outer fence and a 10-foot inner fence completely enclosing the yard" in which he was growing marijuana plants. Undeterred by defendant's efforts, police conducted aerial surveillance over defendant's property. Applying the *Katz* test, the Court held that:

> [I]t is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet. The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.

Id. at 215. By contrast, a cell phone user such as the defendant can easily protect the privacy of location data – literally at the touch of a button – and should not be heard to complain if he fails to do so.

The user agreements and related privacy policies executed by cell phone users with telecommunication providers and smartphone manufacturers provide additional support for the precept that cell phone users knowingly and voluntarily convey geolocation data to those entities. Indeed, as set forth above, those agreements require users to expressly agree that the companies will track their geolocation data and that such data may be provided to Governmental authorities

upon the provision of a subpoena or court order. Based on these facts, it seems that cell phone users voluntarily convey information about their location to third parties, and hence have no reasonable expectation of privacy in this data.

In this case, the issuance of the arrest warrant for the defendant undermines any privacy interest in prospective geolocation data. As the Supreme Court has observed "[b]ecause an arrest warrant authorizes the police to deprive a person of his liberty, it necessarily also authorizes a limited invasion of that person's privacy interest when it is necessary to arrest him in his home." *Steagald v. United States*, 451 U.S. 204, 214 (1981). This is true even though "in terms that apply equally to seizures of property and to seizures of persons, the Fourth Amendment has drawn a firm line at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant." *Id.* at 212 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980). The Fourth Amendment cannot accord protection to geolocation data associated with a defendant's cell phone while denying such protection against a physical invasion of his home, as the latter is entitled to the highest order of defense. *See Payton*, 445 U.S. at 585-86 ("physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed") (quoting *United States v. U.S. District Court*, 407 U.S. 297, 313 (1972)).

Thus, I find that, as to prospective geolocation data, cell phone users who fail to turn off their cell phones do not exhibit an expectation of privacy and such expectation would not be reasonable in any event. This conclusion is supported by the execution of standard industry agreements by which users agree to collection of their geolocation data by third parties, and the provision of such data upon the receipt of a subpoena. Furthermore, the issuance of an arrest warrant for the defendant in this case undermines any expectation of privacy in prospective cell site data. Therefore, under the circumstances, the Government need not obtain a search warrant.

Authorization Order under the Electronic Communications Privacy Act

That the Fourth Amendment does not extend to prospective cell site data does not mean that such information is without legal protection. The disclosure of such information is governed under the procedures established in the Electronic Communications Privacy Act ("ECPA") which provides in relevant part as follows:

> A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction; [or]
>
> (B) obtains a court order for such disclosure under subsection (d) of this section[.]

18 U.S.C. § 2703(c)(1). To obtain a court order under subparagraph (B), the Government must present "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). This is a more demanding standard than that required for a pen register, though less than probable cause. *In re Application of United States*, 620 F.3d 304, 315 (3d Cir. 2010) ("Although the language of § 2703(d) creates a higher standard than that required by the pen register and trap and trace statutes, the legislative history provides ample support for the proposition that the standard is an intermediate one that is less stringent than probable cause"). Thus, it would appear that the Government may obtain prospective cell site authorization either by securing a search warrant or an order under § 2703(d).

However, in defining "electronic communication" for the purposes of the ECPA, Congress specifically excluded "any communication from a tracking device (as defined in section 3117 of this title)." 18 U.S.C. § 2510 (12)(C). That section, in turn, provides as follows:

> Mobile tracking devices
>
> (a) In general.--If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.
>
> (b) Definition.--As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

18 U.S.C. § 3117.

Several courts have denied applications for § 2703(d) orders for cell site information based on the tracking device exclusion, holding that efforts to gain access to prospective cell site information effectively converts an individual's cell phone into a "tracking device." *See, e.g.*, *In re Application*, 849 F. Supp. 2d at 537; *In re Pen Register and Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005) ("communication from a tracking device, such as cell site data, is neither an electronic nor a wire communication under the ECPA, and so it does not fall within the range of covered services provided by an 'electronic service provider'"); *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F. Supp. 2d 294, 311 (E.D.N.Y. 2005) ("the [statutory] definition [of "tracking device"] precisely describes the attribute of the Subject Telephone . . . that renders the disclosure of cell site location information relevant and material to the ongoing investigation").

These cases all depend upon a broad reading of the definition of "tracking device" as contained in the statute. For example, one case explains:

> The ECPA's definition of tracking device is concise and straight-forward: As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or thing. 18 U.S.C. § 3117(b). Aside from its welcome brevity, the definition is striking for its breadth. Note that a device is covered even though it may not have been intended or designed to track movement; it is enough if the device merely

> "permits" tracking. Nor does the definition suggest that a covered device can have no function other than tracking movement. Finally, there is no specification of how precise the tracking must be. Whether from room to room, house to house, neighborhood to neighborhood, or city to city, this unqualified definition draws no distinction.

In re Pen Register, 396 F.Supp.2d at 753. This interpretation ignores the plain meaning of "tracking device" as used to express Congressional intent, contextual information in the statute and logical inconsistencies presented by an unconstrained reading of §3117(b).

First, the phrase "tracking device" had a plain meaning both prior and extrinsic to the enactment of the ECPA in 1986, and has to be viewed against the state of technology as it then existed.[31] The Senate Report accompanying the legislation includes a glossary of terms, among which it provided the following definition of "electronic tracking devices (transponders)":

> These are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such 'homing' devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.

S. Rep. No. 99-541, at 10 (1986). Based on this definition, it would appear that section 3117 incorporated the then-common understanding of tracking device, to wit: a device designed and intended to perform a law enforcement function of tracking an automobile, person or item after being "placed" by agents.[32]

---

[31] In fact, one witness testifying in connection with the bill warned that "[p]resumably, this prohibition is intended to reach only those devices that are used solely or primarily to track persons or objects. However, the definition of the term 'tracking device' in the current bill is broad enough that it could be read as including paging or cellular equipment." *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong. 1 (1986) (statement of John Stanton, Chairman, Telocator Network of America).

[32] At this writing, Congress has undertaken to examine the ECPA with an eye toward amendment in light of subsequent technological developments. *See* Somini Sengupta, *Updating an E-Mail law From the Last Century*, N.Y. Times, Apr. 25, 2013, at B1, *available at* http://www.nytimes.com/2013/04/25/technology/updating-an-e-mail-law-from-the-last-century.html. A refined definition of "tracking device" – among other issues – would provide welcome clarity for courts struggling to apply this legislation.

Second, by focusing solely on subsection (b) of section 3117, this construction ignores subsection (a), which sheds additional light on the meaning of "tracking device" by providing for the device's "installation." This context supports the notion that the statute is aimed at devices installed specifically to track someone or something, as opposed to cell phones which, incidental to their intended purpose, can be tracked or traced.[33]

Lastly, construing "tracking device" to encompass a cell phone is simply illogical and unworkable in this context. For example, under the broader reading, an individual travelling by bicycle, leaving tire tracks in a muddy field; an automobile taillight, which could permit officers to follow a car at night; or the transmitter of a pirate radio station, the signal from which may be located via triangulation, would each constitute an "electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b). That officials opt to follow these clues could not possibly transform the bicycle, taillight or illegal transmitter into a tracking device requiring a search warrant, and such an interpretation would do violence to the clear intent of the statute. Similarly, I find that gathering geolocation information about a cellular telephone does not convert the phone into a "tracking device" for the purpose of the statute. *See In re Application of United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices*, 632 F.Supp.2d 202, 207 (E.D.N.Y. 2008) ("the definition of the phrase "electronic communication" in the SCA, which excludes information from a tracking device, is immaterial to the question of whether the Government may obtain 'a record or other information pertaining to a subscriber or customer of' such an electronic communication service under Section 2703 of the SCA"); *In re Application for an Order Authorizing the*

[33] "This new code section provides that if a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, and the tracking of the object or person on which the device is installed, such warrant remains valid even if the device is moved outside the jurisdiction of the court, even outside the jurisdiction of the United States, provided that the device was installed within the jurisdiction of the court, in conformity with the court order." S. Rep. No. 99-541, at 33-34 (1986).

Extension and use of a Pen Register Device, No. 07-SW-034, 2007 WL 397129, at *2 (E.D. Cal. Feb. 1, 2007) (18 U.S.C. § 3117(b) does not include the acquisition of cell site information in the terms "tracking device").

Thus, because a cell phone does not fall within the "tracking device" exclusion, the Government may properly seek an authorization order for prospective cell site data under section 2703.

CONCLUSION

Because there was probable cause to believe that the prospective geolocation information sought would assist in the location and apprehension of the defendant, a search warrant properly issued. In the alternative, I find that an authorization order properly issued under 18 U.S.C. § 2703, based the specific and articulable facts set forth in the application.

Dated: Central Islip, New York
May 1, 2013

SO ORDERED:

/s/ Gary R. Brown
GARY R. BROWN
United States Magistrate Judge