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

IN THE MATTER OF AN APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE RELEASE OF HISTORICAL CELL-SITE INFORMATION

MEMORANDUM & ORDER

10-MC-897 (NGG)

----------X

NICHOLAS G. GARAUFIS, United States District Judge.

This matter comes before the court as an application for two orders directing Verizon Wireless, a cell-phone service provider, to disclose recorded information of cell-site-location records for one of its customers pursuant to 18 U.S.C. §§ 2703(c)(1), (d) (the "Stored Communications Act" or "SCA"). (See Gov't Letter Appl. (Docket Entry # 5).) An identical application was denied on constitutional grounds by Magistrate Judge James Orenstein on December 23, 2010. (Mag. Order (Docket Entry # 2).) The Government chose to "resubmit the Application" to this court as miscellaneous judge "following its denial by Judge Orenstein." (Gov't Letter Appl. at 2.) In this capacity, the court considers this application de novo and denies it for the reasons set forth below.

I. BACKGROUND

On December 22, 2010, in a sealed application, the Government sought an order pursuant to the SCA. (Sealed Appl. (Docket Entry # 1).) The proposed sealed order directs Verizon Wireless to "disclose recorded information identifying the base station towers and sectors that received transmissions" ("cell-site-locations" or "cell-site-location records") from the target cell phone at the "beginning and the end of calls or text message transmissions . . . for the period from September 1, 2010 until" the day the court issued the proposed order. (Id.) Thus, the proposed order seeks cell-site-location records for a period of at least 113 days. (See Mag. Order

(Docket Entry # 2) at 1.) The Government represented that the phone at issue was registered to and used by an individual who was the target of a criminal investigation. (Sealed Appl. at 1, 5.)

On December 23, 2010, Judge Orenstein denied the Government's application "without prejudice to the government's right to seek similar relief by means of an application for a search warrant pursuant to Federal Rule of Criminal Procedure 41 on the basis of a showing of probable cause." (Mag. Order at 1.) Judge Orenstein concluded that, while the SCA permits the relief sought, "granting the government's application would violate the Fourth Amendment." (Id.) Judge Orenstein's decision in this case incorporated his reasoning in In the Matter of an Application of United States for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578 (E.D.N.Y. 2010). (Mag. Order at 7.)

Following this denial, the Government resubmitted its application for an order to this court on January 11, 2011. (Gov't Letter Appl.) While the court has previously approved similar applications, see In the Matter of an Application of the United States for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices ("In re E.D.N.Y."), 632 F. Supp. 2d 202 (E.D.N.Y. 2008), the court considers anew the constitutionality of ordering this application in light of recent developments in Fourth Amendment jurisprudence.

II. INTRODUCTION

The vast majority of Americans own cell phones. Many Americans have abandoned land line phones entirely, and use cell phones for all telephonic communications. Typically people carry these phones at all times: at work, in the car, during travel, and at home. For many Americans, there is no time in the day when they are more than a few feet away from their cell phones.

Cell phones work by communicating with cell-sites operated by cell-phone service providers. Each cell-site operates at a certain location and covers a certain range of distance. The number of cell-sites that must be placed within a particular area, and thus the distance between cell-sites, is determined by several factors, including population density.

If a user's cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site's geographical range. By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users' cell phones have communicated.

The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night. And under current statutes and law enforcement practices, these records can be obtained without a search warrant and its requisite showing of probable cause.

What does this mean for ordinary Americans? That at all times, our physical movements are being monitored and recorded, and once the Government can make a showing of less-than-probable-cause, it may obtain these records of our movements, study the map our lives, and learn the many things we reveal about ourselves through our physical presence.

Despite the SCA, this court considers whether the Fourth Amendment to the United States Constitution requires a warrant and a showing of probable cause before the Government may obtain the cell-site-location records requested here.

III. LEGAL STANDARD

A. Stored Communications Act

The SCA permits the Government to obtain an order seeking the cell-site-location records requested here. 18 U.S.C. §§ 2703(c)(1), (d); see also In re E.D.N.Y., 632 F. Supp. 2d at 202.

The relevant statutory provision states, "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 . . . obtains a court order for such disclosure under subsection (d) of this section." 18 U.S.C. § 2703(c)(1)(B). Such an order "may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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 showing is lower than the probable cause standard required for a search warrant. See United States v. Maynard, 615 F.3d 544, 566 (D.C. Cir. 2010) (citing Katz v. United States, 389 U.S. 347, 357 (1967)). Thus, this court must consider whether granting the requested order on this lower-than-probable-cause standard is consistent with the Fourth Amendment.

B. Fourth Amendment

The Fourth Amendment guarantees that "[t]he 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 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." U.S. Const. amend. IV. "A search conducted without a warrant is 'per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'" Maynard, 615 F.3d at 566 (quoting Katz, 389 U.S. at 357). Thus, if obtaining the records sought by the Government here constitutes a search as defined by the Fourth

Amendment, it is presumed that the Government must, at a minimum, obtain a warrant on a showing of probable cause.

Whether Government action constitutes a search depends upon whether "the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." Smith v. Maryland, 442 U.S. 735, 740 (1979). The Supreme Court in Katz v. United States set forth a two part standard for when a Fourth Amendment search has occurred: (1) the individual has "manifested a subjective expectation of privacy" in the thing searched; and (2) "society is willing to recognize that expectation as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001). The first element addresses whether the individual's conduct has "exhibited an actual (subjective) expectation of privacy . . . [which is demonstrated by] whether . . . the individual has shown that he seeks to preserve something as private." United States v. Knotts, 460 U.S. 276, 281 (1981) (internal citations and quotation marks omitted). The second element looks to whether the "individual's expectation, viewed objectively, is justifiable under the circumstance." Id. (internal citations and punctuation omitted).

The Katz test applies to all searches, including searches pertaining to the home, which are at the core of the Fourth Amendment. See Kyllo, 533 U.S. at 31-33 (citing Smith, 442 U.S. at 743-44 (applying the Katz factors to hold that it is not a search for the government to track phone numbers dialed, even if they are dialed from a private home)); California v. Ciraolo, 476 U.S. 207, 211-15 (1986) (applying Katz factors and holding that, generally, aerial surveillance of private homes and surrounding areas is not a search)).

C. Constitutionality of Electronic Surveillance of Location

Electronic surveillance of an individual's location as he travels in public has traditionally not been construed as a Fourth Amendment search, although electronic surveillance of his location within his home has been. See Knotts, 460 U.S. at 280-85; United States v. Karo, 468 U.S. 705, 713-18 (1984). Reading United States v. Knotts broadly, courts have concluded that individuals have no reasonable expectation of privacy over their location for all travels in public spaces. See, e.g., United States v. Garcia, 474 F.3d 994, 996-99 (7th Cir. 2007) (holding that Global Positioning Satellite ("GPS") tracking by law enforcement of an individual's vehicle does not constitute a Fourth Amendment search). This broad reading of Katz, however, has been recently challenged by case law on electronic surveillance. See Maynard, 615 F.3d at 555-68; United States v. Pineda-Moreno ("Pineda-Moreno II"), 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, J., dissenting) ("The Supreme Court in Knotts expressly left open whether twenty-four hour surveillance of any citizen of this country by means of dragnet-type law enforcement practices violates the Fourth Amendment's guarantee of personal privacy. When requests for cell phone location information have become so numerous that the telephone company must develop a self-service website so that law enforcement agents can retrieve user data from the comfort of their desks, we can safely say that such dragnet-type law enforcement practices are already in use. This is precisely the wrong time . . . to say that the Fourth Amendment has no role to play in mediating the voracious appetites of law enforcement." (internal citations and quotation marks omitted)).

In Knotts, the Supreme Court addressed the constitutionality of electronic surveillance of an individual's location. 460 U.S. at 280-85. The Court considered the narrow question of whether warrantless tracking-beeper-aided surveillance of a car traveling on public roads from

one location to another violated the Fourth Amendment. The Court ruled that it did not, holding that "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements *from one place to another*" because "he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property." Knotts, 460 U.S. at 281-82 (emphasis added). The fact that electronic tracking technology was employed to facilitate this surveillance did not change the Court's analysis. Id. at 282.

Knotts explicitly left unresolved whether electronic surveillance of movements in public for an extended period can constitute a search, even though electronic surveillance of movements in public from one place to another does not. Knotts, 460 U.S. at 284. In so doing, the Court noted that if "dragnet type law enforcement practices" such as "twenty-four hour surveillance of any citizen . . . without judicial knowledge or supervision" should occur, "there will be time enough then to determine whether different constitutional principles may be applicable." Id. (internal citation and quotation marks omitted).

Shortly after Knotts, the Supreme Court considered "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." Karo, 468 U.S. 713-18. There, the Court held that use of an electronic tracking device *does* constitute a Fourth Amendment search if the tracking device enables the Government to "obtain information that it could not have obtained by observation from outside the curtilage of the house." Id. at 715. Read together, Karo and Knotts stand for the proposition that the Government's obtaining of some electronically collected location information constitutes a search under the Fourth

Amendment depending on the location (Karo) and, potentially, quantity (Knotts) of that information.

The Court of Appeals for the District of Columbia Circuit has since addressed the constitutionally of continual surveillance left unresolved by Knotts. Maynard, 615 F.3d at 555-68, cert. granted, United States v. Jones, 2011 WL 1456728, *1 (U.S. 2011). In United States v. Maynard, the Government attached a GPS tracking device to the defendant's vehicle without a warrant and tracked his movements in the vehicle at all times for four weeks. Id. at 555. The Maynard court held that this prolonged electronic surveillance of an individual's location constituted a Fourth Amendment search. Id. at 555-68. But see United States v. Pineda-Moreno ("Pineda-Moreno I"), 591 F.3d 1212, 1216-17 (9th Cir. 2010); Garcia, 474 F.3d at 996-99.

The Maynard court noted two important distinctions between the short-term surveillance in Knotts and the prolonged surveillance at issue in Maynard. First, the court concluded that while the individual in Katz did not have a reasonable expectation of privacy over his location while traveling from one place to another, the individual in Maynard had a reasonable expectation of privacy over the *totality* of his movements over the course of a month. The court reasoned that the totality of one's movements over an extended time period is not actually exposed to the public "because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil." Maynard, 615 F.3d at 560. Second, the court concluded that people have an objectively reasonable expectation of privacy in the totality of their movements over an extended period because an individual's privacy interests in the totality of his movements far exceeds any privacy interest in a single public trip from one place to another.

> The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction

> between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more . . . .
>
> . . . Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.

Id. at 561-62. Finally, the court concluded that society recognizes an individual's "expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation." Id. at 563.

Here, the Government has requested what is essentially at least 113 days of constant surveillance of an individual. (Sealed Appl.) Following Maynard's persuasive reasoning, this court concludes that the application seeks information that is protected by the Fourth Amendment. The proposed sealed order directs the cell-phone service provider to "disclose recorded information identifying the base station towers and sectors that received transmissions" from the target telephone at the "beginning and the end of calls or text message transmissions . . . for the period from September 1, 2010 until" the day the court issues the proposed order, which was at least December 22, 2010, when the application was submitted to Judge Orenstein, or January 11, 2011, when submitted to this court. The cell-site-location records sought here captures enough of the user's location information for a long enough time period—significantly

longer than the four weeks in Maynard—to depict a sufficiently detailed and intimate picture of his movements to trigger the same constitutional concerns as the GPS data in Maynard.

In fact, cell-site-location records present even greater constitutional concerns than the tracking at issue in Maynard. Even United States Courts of Appeals that have approved the form of electronic tracking at issue in Maynard, have noted that mass electronic surveillance presents greater constitutional concerns. For example, in United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) the court noted,

> It is imaginable that a police unit could undertake "wholesale surveillance" by attaching such devices to thousands of random cars and then analyzing the volumes of data produced for suspicious patterns of activity. Such an effort, if it ever occurred, would raise different concerns than the ones present here. In this case, there was nothing random or arbitrary about the installation and use of the device.

Marquez, 605 F.3d at 610 (internal citation omitted). In Pineda-Morena I, the court stated,

> We, like the Seventh Circuit, believe that should the government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.

Pineda-Morena I, 591 F.3d at 1217 n.2 (internal citations and punctuation omitted). Similarly, in Garcia, the Court noted in dicta that while GPS surveillance on one car did not constitute a Fourth Amendment search,

> new technologies enable, as the old (because of expense) do not, wholesale surveillance. . . . It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation's roads. . . . Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive. Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case.

Garcia, 474 F.3d at 998. The cell-site-location records at issue here currently enable the tracking of the vast majority of Americans. Thus, the collection of cell-site-location records effectively enables "mass" or "wholesale" electronic surveillance, and raises greater Fourth Amendment concerns than a single electronically surveilled car trip. This further supports the court's conclusion that cell-phone users maintain a reasonable expectation of privacy in long-term cell-site-location records and that the Government's obtaining these records constitutes a Fourth Amendment search.

D. Third-Party-Disclosure Doctrine

While the court concludes that cell-phone users have a reasonable expectation of privacy in their long-term cell-site-location records, the court must consider whether cell-phone users nonetheless destroy this expectation of privacy by communicating their location information to the cell-phone service provider by carrying and using a cell phone.

Under the Fourth Amendment, a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," Smith, 442 U.S. at 743-44, a principle known as the "third-party-disclosure doctrine." The Supreme Court has reasoned that when a person reveals some information to a third party, they assume the risk that the third party may disclose it to the Government. See Smith, 442 U.S. at 742-46. As a result, the Fourth Amendment does not prohibit the Government from obtaining information disclosed to a third party because any reasonable expectation of privacy is destroyed when the risk of disclosure is assumed. See id.

Courts have applied the third-party-disclosure doctrine to a broad array of factual circumstances. See, e.g., id. (holding that disclosure of phone numbers by dialing them to the phone company eliminates any legitimate expectation of privacy against the phone company

revealing such numbers to the Government); United States v. Miller, 425 U.S. 435, 440-43 (1976) (holding that a Fourth Amendment search does not occur when the Government obtains from banks records including checks, deposit slips, and other information conveyed by bank customers to their banks because this information is "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business"); United States v. Forrester, 512 F.3d 500, 509-12 (9th Cir. 2008) (holding that a computer user has no legitimate expectation of privacy in the to/from addresses of email messages sent from, and the internet protocol ("IP") addresses visited by, a defendant on his home computer because they are conveyed to his service provider).

In Smith v. Maryland, the Court addressed a scenario that is factually similar to the search of cell-site-location records at issue here. The Court held that the Government did not conduct a Fourth Amendment search when it installed a pen register device with a phone service provider to collect phone numbers dialed by the target home phone. Smith, 442 U.S. at 739-46. It reasoned that a telephone subscriber has no reasonable expectation of privacy in records of the numbers dialed from his telephone because

> [a]ll 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. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies for the purposes of checking billing operations, detecting fraud and preventing violations of law.

Id. at 742 (internal citations and quotation marks omitted). Therefore, when people use their phones, they "voluntarily convey[] numerical information to the telephone company and 'expose[]' that information to its equipment in the ordinary course of business. In so doing,

[they] assume[] the risk that the company w[ill] reveal to police the numbers [they] dialed." Id. at 744.

Pursuant to the third-party-disclosure doctrine, it could be argued that an individual "voluntarily" conveys his cell-phone's location to a third party—his service provider—by turning his phone on and making and receiving calls and text messages. As such, several district court and magistrate judges have concluded that cell-phone users have no reasonable expectation of privacy in their cell-site-location records. See, e.g., In re Application of United States for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace ("In re Application: S.D.N.Y."), 405 F. Supp. 2d 435, 449-50 (S.D.N.Y. 2005) (holding that because the cell-phone user "has chosen to carry a device and to permit transmission of its information to a third party . . . the provision of information to a third party does not implicate the Fourth Amendment").

Some other courts have concluded, unpersuasively, that cell-site-location records should be treated differently than the dialing of phone numbers in Smith due to differences in how "knowingly" or "voluntarily" the information is conveyed. For example, the Court of Appeals for the Third Circuit stated that

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

In the Matter of Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 317-18 (3d Cir. 2010). This definition relies too heavily on cell-phone users remaining unaware of the capacities

of cellular technology, a doubtful proposition in the first place. Public ignorance as to the existence of cell-site-location records, however, cannot long be maintained. Rather the expectation of privacy in cell-site-location records, if one exists, must be anchored in something more permanent—it must exist despite the public's knowledge that these records are collected by their service providers.

Providing a more fulsome, albeit hyper-technical, distinction between phone-number and cell-site-location records, Magistrate Judge Stephen Wm. Smith of the Southern District of Texas has emphasized the difference between the methods through which phone numbers and cell-site-location records are conveyed to the service providers:

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

In re Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010).

Nothing in the case law, however, supports the conclusion that any minor technical distinction between the dialing a phone number and the conveyance of cell-site-location records on a cell phone is constitutionally significant. See Smith, 442 U.S. at 743-46. While cell-phone users do not technically convey their location, they do voluntarily convey their cell-phone signal to the cell towers, and expose that information to cell-phone service provider's equipment in the

ordinary course of business. Thus, if no exception to the third-party-disclosure doctrine applies to the present case, then the court would conclude that the cell-phone user, by choosing to carry, turn on, and make and receive communications from a cell phone voluntarily discloses information about his location to a third party. Under the third-party-disclosure doctrine, such a disclosure would eliminate a reasonable expectation of privacy.[1]

As addressed below, however, the court concludes an exception to the third-party-disclosure doctrine should be applied to *cumulative* cell-site-location records.

E. Limitations of Third Party Disclosure Doctrine: Distinction Based upon Intrusiveness and Normative Privacy Concerns

The Supreme Court and lower appellate courts have recognized an exception to the third-party-disclosure doctrine in a subset of cases in which the content of the information communicated would be revealed through the Government's surveillance ("content exception"). Courts have not been transparent about the foundation or contours of this content exception. Its origin, however, almost certainly lies in Ex parte Jackson, 96 U.S. 727, 732-33 (1877). In Jackson and subsequent cases, the Supreme Court established the rule that, despite the fact that letters are turned over to mail carriers, the contents of sealed envelopes sent via first class mail are afforded Fourth Amendment protection until opened by the recipient. 96 U.S. at 732-33. The addressing information and other information written on the outside of the envelope, however, is afforded no such protection. Id.

---

[1] The Katz test and the third-party-disclosure doctrine apply to searches involving the home. See, e.g., Kyllo, 533 U.S. at 31-33 (citing Smith, 442 U.S. at 743-44 (applying Katz factors to hold that it is not a search for the government to track phone numbers dialed, even if they are dialed from a private home); Ciraolo, 476 U.S. at 211-15 (applying Katz factors and holding that, generally, aerial surveillance of private homes and surrounding areas is not a search)). Consequently, if the third-party-disclosure doctrine applied to cell-site-location records, then the fact that cell-site-location records may show movements within the home would provide no additional basis for finding that the Government's collection of cell-site-location data constitutes a Fourth Amendment search, regardless of the Supreme Court's holding in Karo. See In re Application: S.D.N.Y., 405 F. Supp. 2d at 449 (distinguishing cell-site-location records cases from the facts of Karo because, unlike in Karo where the Government installed the tracking device, in cell-site-location records cases the "individual has chosen to carry a device and to permit transmission of its information to a third party").

The content exception was incorporated, by dicta, into Fourth Amendment telephonic communications case law in Smith. 442 U.S. at 741. There, the Court distinguished a pen register device from the listening device at issue in Katz on the grounds that, unlike listening devices, "pen registers do not acquire the *contents* of communications." Smith, 442 U.S. at 741. The Court cited as relevant the limited information that a pen register could record:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.

Id. From these facts, the Court reasoned that, "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." Id. at 742 (internal citations and quotation marks omitted). This reasoning implies that if pen registers recorded the contents of the communication, or even information such as whether a communication occurred, then a reasonable expectation of privacy may be preserved regardless of the communication's disclosure to the third-party phone company. Thus, a finding of third-party disclosure does not necessarily destroy the reasonable expectation of privacy in all circumstances.

The content exception preserves the reasonable expectation of privacy, and thus Fourth Amendment protection, for some information to which strict application of the Katz test and the third-party-disclosure doctrine would not permit. Carving this exception out of the Katz test is consistent with Supreme Court precedent, which has long recognized that the Katz test may fail to provide sufficient Fourth Amendment protections in some cases. See, e.g., Kyllo, 533 U.S. at 34 (noting that "[t]he Katz test—whether the individual has an expectation of privacy that

society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable" (internal citations and quotation marks omitted)). The Court in Smith similarly recognized that the subjective and reasonable expectations of privacy have limitations:

> Situations can be imagined, of course, in which Katz' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

442 U.S. at 741 n.5. As this demonstrates, there are circumstances in which the legal interest being protected from government intrusion trumps any actual belief that it will remain private. In such cases, society's recognition of a particular privacy right as important swallows the discrete articulation of Fourth Amendment doctrine in Smith.[2] As addressed below, the court concludes that the "normative inquiry" envisioned in Smith is required here, and it preserves the reasonable expectation of privacy in cumulative cell-site-location records.

[2] Scholars have argued that courts, including the Supreme Court in Smith, weigh the level of intrusiveness of the search in order to determine if there is a reasonable expectation of privacy. See, e.g., Renée McDonald Hutchins, Tied Up in Knotts? GPS Technology and the Fourth Amendment, 55 UCLA L. Rev. 209, 430-44 (2007). Under this theory, the results in Smith and Katz can be explained by the fact that the disclosure of telephone numbers was not sufficiently intrusive to constitute a Fourth Amendment search, while the recording of the contents of a phone conversation in Katz was. This content exception, thus, represents one application of the broader intrusiveness analysis. Intrusiveness analysis, therefore, can be applied to extend the treatment afforded in the case law to content to other highly intrusive information, such as cell-site-location records.

Recently, courts have applied the content exception to extend Fourth Amendment protection to new communication technologies such as email, text messaging, and internet search.[3] For example, in United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), the Court of Appeals for the Sixth Circuit held that an email subscriber "enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP" such that "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause."[4] In arriving at this conclusion, the court held that "the ISP's control over the emails and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy." Warshak, 631 F.3d at 287.[5] The opinions in Warshak, United States v. Quon, 529 F.3d at 903-08, and United States v. Forrester, 512 F.3d at 509-12 demonstrate that courts have applied the content exception to the third-party-disclosure doctrine in order to preserve the reasonable

[3] In United States v. Quon, 529 F.3d 892, 903-08 (9th Cir. 2008), rev'd on other grounds, California v. Quon, 130 S. Ct. 2619, 2630 (2010), the Court of Appeals for the Ninth Circuit held that users of text messaging services have a reasonable expectation of privacy in their text messages stored on the service provider's network. The Quon court held that the fact the service provider "may have been able to access the contents of the messages for its own purposes is irrelevant" because the phone user "did not expect that [the service provider] would monitor their text messages, much less turn over the messages to third parties without Appellants' consent." Id. at 905-06; see also Forrester, 512 F.3d at 509-12 (holding that collection from internet service providers of the to/from addresses of email messages sent from, and the internet protocol ("IP") addresses visited by, a defendant on his home computer does not constitute a fourth amendment search, but noting that had the requested information revealed the contents of the email communication or the internet search text contained in the URL, a different result may be required because, "the contents may deserve Fourth Amendment protection, but the address and size of the package do not.").

[4] The only case in which the Court of Appeals for the Second Circuit has addressed the reasonable expectation of privacy in email is United States v. Lifshitz, 369 F.3d 173, 190 (2004). There, the court stated, in dicta and without further explanation, that while individuals generally possess "a reasonable expectation of privacy in their home computers . . . [t]hey may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient." Lifshitz, 369 F.3d at 190. The court in Lifshitz, however, did not apply the typical Fourth Amendment standards because that case involved search terms imposed on a probationer, and probationers have significantly diminished privacy expectations. Id. Thus, this dicta in Lifshitz provides this court little guidance under the circumstance presented here.

[5] The Warshak court distinguished email from the bank records in Miller on two grounds: (1) "Miller involved simple business records, as opposed to the potentially unlimited variety of 'confidential communications' at issue here"; (2) "the bank depositor in Miller conveyed information to the bank so that the bank could put the information to use 'in the ordinary course of business.' By contrast, [the email recipient] received his emails through [the service provider]. [The service provider] was an intermediary, not the intended recipient of the emails." Id. at 288.

expectation of privacy to users of new forms of communication technology that expose what society regards as highly private information.

While each of these recent cases nominally applies the content exception, there is no meaningful Fourth Amendment distinction between content and other forms of information, the disclosure of which to the Government would be equally intrusive and reveal information society values as private. See Smith, 442 U.S. at 741 n.5. Consequently, the court concludes an exception to the third-party-disclosure doctrine applies to cell-site-location records for the following reasons.

First, the case law supports applying an exception to the third-party-disclosure doctrine here because the information is disclosed to a service-provider intermediary, as it was in Smith, Warshak, Quon, and Forester. Limiting the application of exceptions to the third-party-disclosure doctrine to cases involving disclosure to service-provider intermediaries is consistent with existing Fourth Amendment doctrine. Such a limited application would preserve the third-party-disclosure doctrine in typical cases where information is disclosed to third parties, such as consensual surveillance cases, See Smith, 442 U.S. at 749-50 (Marshall, J., dissenting) (collecting cases); and in cases where the information disclosed to the service-provider intermediary does not implicate sufficient privacy concerns, like the telephone numbers dialed in Smith; while enabling Fourth Amendment protections to be extended to users of some of the many new and widely used communication technologies in which service-provider intermediaries receive and store private user information incident to service.[6]

---

[6] In an article addressing the application of the third-party-disclosure doctrine to internet communications, Orin Kerr, has argued that while

> [t]he Supreme Court has never explicitly stated why the third-party doctrine should not apply in the [phone conversation interception scenario addressed in Katz]. . . . [T]he key point is that the third-party doctrine has not been extended to *intermediaries* that merely send and receive contents without needing to access or analyze those communications. Instead, courts have widely adopted

Second, the court concludes that established normative privacy considerations support the conclusion that the reasonable expectation of privacy is preserved here, despite the fact that cell-site-location records is disclosed to cell-phone service providers. Applying the third-party-disclosure doctrine to cumulative cell-site-location records would permit governmental intrusion into information which is objectively recognized as highly private. See Maynard, 615 F.3d at 555. Following the decision in Maynard, this court concludes that cumulative cell-site-location records implicate sufficiently serious protected privacy concerns that an exception to the third-party-disclosure doctrine should apply to them, as it does to content, to prohibit undue governmental intrusion.[7] Consequently, the court concludes that an exception to the third-party-disclosure doctrine applies here because cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records, despite the fact that those records are collected and stored by a third party.

F. Effects of Changing Technology on the Fourth Amendment

In order to prevent the Fourth Amendment from losing force in the face of changing technology, Fourth Amendment doctrine has evolved throughout time and must continue to do so. See, e.g., Kyllo 533 U.S. at 33-34 (ruling that the use of heat sensing technology to detect

---

the content/non-content line or a functional equivalent in cases applying the Fourth Amendment to communications networks.

Orin S. Kerr, Applying the Fourth Amendment to the Internet: A General Approach, 62 Stan. L. Rev. 1005, 1038 (2010) (emphasis added). While this analysis partially explains courts' application of the third-party doctrine in cases in which information is received by intermediaries, the "without needing to access or analyze those communications" caveat appears too narrow to accommodate current case law and the realities of current technology. For example, would the third-party doctrine remove the reasonable expectation of privacy over the contents of emails sent on Gmail, or similar email providers, that use computers to access and analyze the contents of email communications in order to display advertisements? While the court need not answer the question here, it appears that such a technology-specific definition of third-party disclosure would fail to take into account the importance of the information disclosed or the intrusive nature of disclosing such information.

[7] While it was not necessary to its holding, the Supreme Court in City of Ontario, California v. Quon, 130 S. Ct. 2619, 2630 (2010), noted that "cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy." This further supports the conclusion that Americans view the expectation of privacy in certain aspects of one's cell-phone communication as normatively reasonable.

activity inside the home was unconstitutional and noting that this rule "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted"). Like in Kyllo, the court here confronts the question of what "limits there are upon this power of technology to shrink the realm of guaranteed privacy." Id. at 33. The advent of technology collecting cell-site-location records has made continuous surveillance of a vast portion of the American populace possible: a level of Governmental intrusion previously inconceivable. It is natural for Fourth Amendment doctrine to evolve to meet these changes.

The Supreme Court in Katz, after all, drastically changed existing Fourth Amendment doctrine in concluding that the phone booth user had a reasonable expectation of privacy over the contents of his conversation. Smith, 389 U.S. at 348-59. In changing existing Fourth Amendment doctrine in order to accommodate changes in technology, the Court noted that "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." Id. at 352. The cell phone has replaced the public telephone to near extinction; yet, to date Fourth Amendment doctrine has not developed to embrace the vital role the cell phone has come to play in private communication and the new Fourth Amendment challenges in creates.

The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by "choosing" to carry a cell phone must be rejected. In light of drastic developments in technology, the Fourth Amendment doctrine must evolve to preserve cell-phone user's reasonable expectation of privacy in cumulative cell-site-location records.

The Supreme Courts has warned that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has

become clear." Quon, 130 S. Ct. at 2630. This court, however, does not set out here to "establish far-reaching premises that define the existence, and extent, of privacy expectations." Id. (internal citations omitted)). Rather, it only seeks to resolve the question before it: whether the request for at least 113 days of cumulative cell-site-location records for an individual's cell phone constitutes a search under the Fourth Amendment. (Sealed Appl. at 1, 5.) The court concludes that it does. Consequently, the information sought by the Government may not be obtained without a warrant and the requisite showing of probable cause. The Government's motion is denied without prejudice to any future applications seeking to obtain the requested information through a warrant pursuant to 18 U.S.C. §§ 2703(c)(1)(a) and Federal Rule of Criminal Procedure 41.

IV. CONCLUSION

While the government's monitoring of our thoughts may be the archetypical Orwellian intrusion, the government's surveillance of our movements over a considerable time period through new technologies, such as the collection of cell-site-location records, without the protections of the Fourth Amendment, puts our country far closer to Oceania than our Constitution permits. It is time that the courts begin to address whether revolutionary changes in technology require changes to existing Fourth Amendment doctrine. Here, the court concludes only that existing Fourth Amendment doctrine must be interpreted so as to afford constitutional protection to the cumulative cell-site-location records requested here. For the foregoing reasons the Government's motion for orders pursuant to 18 U.S.C. § 2703(c)(1) and (d) is DENIED.

SO ORDERED.

s/Nicholas G. Garaufis

Dated: Brooklyn, New York
August 22, 2011

NICHOLAS G. GARAUFIS
United States District Judge