UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE: APPLICATION FOR TELEPHONE INFORMATION NEEDED FOR A CRIMINAL INVESTIGATION

Case No. 15-XR-90304-HRL-1(LHK)

ORDER AFFIRMING DENIAL OF APPLICATION FOR HISTORICAL CELL SITE LOCATION INFORMATION

[PUBLIC REDACTED VERSION]

Before the Court is the government's appeal of U.S. Magistrate Judge Howard R. Lloyd's denial of an application for an order pursuant to 18 U.S.C. § 2703(d) authorizing the government to obtain historical cell site location information ("CSLI") associated with [redacted] target cell phones. ECF No. 4 ("Gov't Br."); ECF No. 5 ("Gov't Supp. Br.").[1] The Federal Public Defender for the Northern District of California ("Public Defender"), at the Court's invitation, filed a response. ECF No. 21 ("Opp."). With the Court's permission, the American Civil Liberties Union ("ACLU") and the Electronic Frontier Foundation ("EFF") filed amicus briefs in support of the

[1] The government does not appeal Judge Lloyd's ruling to the extent he denied the government's application for prospective CSLI. *See* Gov't Br. at 1. The Court's analysis is therefore confined to historical CSLI only.

Public Defender. ECF No. 19 ("ACLU Br."); ECF No. 20 ("EFF Br."). The government replied. ECF No. 22 ("Gov't Reply"). Having considered these written submissions, the relevant law, the record in this case, and the oral arguments presented at the June 24, 2015 hearing, the Court hereby AFFIRMS Judge Lloyd's denial of the government's application for historical CSLI.

I. BACKGROUND

A. Cell Phone Technology and CSLI

Cell phones operate through the use of radio waves. To facilitate cell phone use, cellular service providers maintain a network of radio base stations—also known as cell towers—throughout their coverage areas. *See Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance, Hearing Before the Subcomm. on Crime, Terrorism, Homeland Security, and Investigations, of the H. Comm. on the Judiciary,* 113th Cong. 50 (2013) (written testimony of Prof. Matt Blaze, University of Pennsylvania) ("Blaze Testimony"), *available at* http://www.judiciary.house.gov/index.cfm?a=Files.Serve&File_id=91FBF844-052E-4743-9CCE-19168FA815D2. Most cell towers have multiple cell sectors (or "cell sites") facing in different directions. ECF No. 22-1, Declaration of Special Agent Hector M. Luna ("Luna Decl.") ¶ 3A. A cell site, in turn, is a specific portion of the cell tower containing a wireless antenna, which detects the radio signal emanating from a cell phone and connects the cell phone to the local cellular network or Internet. Blaze Testimony at 50. For instance, if a cell tower has three antennas, each corresponding cell site would service an area within a 120-degree arc. *See* Thomas A. O'Malley, *Using Historical Cell Site Analysis Evidence in Criminal Trials*, U.S. Att'y Bull., Nov. 2011, at 19, *available at* http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf.

Whenever a cell phone makes or receives a call, sends or receives a text message, or otherwise sends or receives data, the phone connects via radio waves to an antenna on the closest cell tower, generating CSLI. The resulting CSLI includes the precise location of the cell tower and cell site serving the subject cell phone during each voice call, text message, or data

connection. Luna ¶ 3A. If a cell phone moves away from the cell tower with which it started a call and closer to another cell tower, the phone connects seamlessly to that next tower. Blaze Testimony at 50.

Significantly, the government's special agent from the Federal Bureau of Investigation ("FBI") informs the Court that CSLI may be generated in the absence of user interaction with the cell phone. Luna Decl. ¶ 3B. For example, CSLI may still be generated during an incoming phone call that is not answered. *Id.* Additionally, most modern smartphones have applications that continually run in the background, sending and receiving data without a user having to interact with the cell phone. *Id.*

Indeed, cell phones, when turned on and not in airplane mode, are always scanning their network's cellular environment. Luna Decl. ¶ 3B. In so doing, cell phones periodically identify themselves to the closest cell tower—i.e., the one with the strongest radio signal—as they move throughout their network's coverage area. Blaze Testimony at 50. This process, known as "registration" or "pinging," facilitates the making and receiving of calls, the sending and receiving of text messages, and the sending and receiving of cell phone data. *See id.* Pinging is automatic and occurs whenever the phone is on, without the user's input or control. U.S. Dep't of Homeland Sec., *Lesson Plan: How Cell Phones Work* 9 (2010) ("DHS Lesson Plan"), *available at* https://www.eff.org/files/filenode/3259_how_cell_phones_work_lp.pdf. A cell phone that is switched on will ping the nearest tower every seven to nine minutes. *Id.* At oral argument, the Court was informed that at least some cellular service providers keep track of the CSLI generated by registration "pings." Hr'g Tr. at 4:19-5:6.

As the number of cell phones has increased, the number of cell towers—and thus cell sites—has increased accordingly:

> A sector can handle only a limited number of simultaneous call connections given the amount of radio spectrum "bandwidth" allocated to the wireless carrier. As the density of cellular users grows in a given area, the only way for a carrier to accommodate more customers is to divide the coverage area into smaller and smaller sectors, each served by its own base station and antenna. New services, such as 3G and LTE/4G Internet create additional pressure on the available

> spectrum bandwidth, usually requiring, again, that the area covered by each sector be made smaller and smaller.

Blaze Testimony at 54. Densely populated urban areas therefore have more cell towers covering smaller geographic locations. For example, the Public Defender informs the Court that within three miles of the San Jose Federal Courthouse, there are 199 towers (with applications for three more currently pending) and 652 separate antennas. Opp. at 3. Within just one mile of the Federal Courthouse in New York City, there are 118 towers and 1,086 antennas. *Id.*

In addition to the large, three-sided cell towers, smaller and smaller base stations are becoming increasingly common. Examples include microcells, picocells, and femtocells, all of which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home. Blaze Testimony at 43-44. This proliferation of base stations to cover smaller areas means that "knowing the identity of the base station (or sector ID) that handled a call is tantamount to knowing a phone's location to within a relatively small geographic area . . . sometimes effectively identifying individual floors and rooms within buildings." *Id.* at 55-56. Although the ability of cellular service providers to track a cell phone's location within an area covered by a particular cell site might vary, it has become ever more possible for the government to use CSLI to calculate a cell phone user's "locations with a precision that approaches that of GPS." *Id.* at 53.

The government acknowledged as much at oral argument, conceding that CSLI has gotten more precise over the years. Hr'g Tr. at 32:5-9. The fact is new tools and techniques are continually being developed to track CSLI with greater precision. Cellular service providers, for instance, can triangulate the location of a cell phone within an area served by a particular cell site based on the strength, angle, and timing of that cell phone's signal measured across multiple cell site locations. Blaze Testimony at 56.

Lastly, the volume of location data generated by an individuals' cell phone can be immense, as the ACLU points out. *See* ACLU Br. at 5-7; ECF No. 19-1, Declaration of Nathan Freed Wessler ("Wessler Decl."). For example, in *United States v. Carpenter*, a case now pending

in the Sixth Circuit and arising out of the greater Detroit area, the government obtained 127 days of CSLI for one defendant, Timothy Carpenter, and 88 days of CSLI for another, Timothy Sanders. *See United States v. Carpenter*, No. 14-1572 (6th Cir. filed May 7, 2014). Carpenter's data include 6,449 separate call records for which CSLI was logged, comprising 12,898 cell site location data points. *See* Wessler Decl. ¶ 8. Sanders's records reveal 11,517 calls for which location information was logged, comprising 23,034 cell site location data points. *Id.* ¶ 9. Carpenter and Sanders, respectively, placed or received an average of 50.8 and 130.9 calls per day for which location data was recorded and later obtained by the government. *Id.* ¶ 10. For Carpenter, that amounts to an average of 102 location points per day, or one location point every 14 minutes. For Sanders, it amounts to an average of 262 location points per day, or one location point every six minutes.

B. Statutory Framework

An application for historical CSLI is governed by the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, which was enacted in 1986 as Title II of the Electronic Communications Privacy Act ("ECPA"). The SCA covers the disclosure of communication information by providers of electronic communications, including cellular service providers. Section 2703(a) covers circumstances in which a government entity may require such providers to disclose the *contents* of wire or electronic communications in electronic storage, while § 2703(b) covers circumstances in which a government entity may require providers to disclose the *contents* of wire or electronic communications held by a remote computing service. *See id.* § 2703(a)-(b). Neither of these provisions is at issue here.

Instead, the government seeks what is referred to in § 2703(c) as "a record or other information pertaining to a subscriber to or customer of [a provider of electronic communication service]," a term that expressly excludes the contents of communications. 18 U.S.C. § 2703(c)(1). Although the SCA makes no mention of historical CSLI, there is no dispute that the historical CSLI sought by the government qualifies as a stored "record or other information pertaining to a

subscriber . . . or customer," and therefore falls within the scope of § 2703(c)(1). As relevant here, § 2703(c) provides:

> c) Records concerning electronic communication service or remote computing service.—
>
> (1) 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 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
>
> (B) obtains *a court order* for such disclosure *under subsection (d)* of this section.

Id. § 2703(c)(1)(A)-(B) (emphases added).

In submitting its request to Judge Lloyd in this case, the government did not seek to obtain a warrant under § 2703(c)(1)(A). Rather, the government sought a court order under § 2703(d), as authorized by § 2703(c)(1)(B). The requirements for a court order under § 2703(d) are as follows:

> (d) Requirements for court order.—
>
> A court order for disclosure under subsection (b) or (c) 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*. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C. § 2703(d) (emphasis added). The "specific and articulable facts" standard set forth in § 2703(d) requires a showing that is less than probable cause. *See, e.g., United States v. Davis*, 785 F.3d 498, 505 (11th Cir. 2015) (explaining that "[§ 2703(d)'s] statutory standard is less than the probable cause standard for a search warrant"); *In re U.S. for Historical Cell Site Data* ("*Fifth Circuit Opinion*"), 724 F.3d 600, 606 (5th Cir. 2013) ("The 'specific and articulable facts' standard is a lesser showing than the probable cause standard that is required by the Fourth

Amendment to obtain a warrant."); *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't* ("*Third Circuit Opinion*"), 620 F.3d 304, 315 (3d Cir. 2010) (explaining that the § 2703(d) standard is "less stringent than probable cause").

C. Government's Application

The government's application seeks historical CSLI associated with [redacted] target cell phones for a period of sixty days prior to the date on which the application is granted. App. ¶¶ 1, 2a. According to the application, the requested CSLI includes "the physical location and/or address of the cellular tower and identification of the particular sector of the tower receiving the signal." *Id.* ¶ 2a n.4. "This information," the application says, "does not provide the specific or precise geographical coordinates of the [target cell phone]," nor does it include "the contents of communications." *Id.* ¶ 2a & n.4. In addition, the application "does not seek" (1) CSLI "that might be available when the [target cell phones] are turned 'on' but a call is not in progress"; (2) information regarding the strength, angle, and timing of a target cell phone's signal measured at two or more cell site locations "that would allow the government to triangulate" a target cell phone's precise location; and (3) a target cell phone's GPS information, "even if that technology is built in." *Id.* ¶ 3 (footnote omitted). The application's reference to a "call," as the government confirmed at the hearing, includes phone calls, text messages, and data connections. Hr'g Tr. at 50:22-52:5. In sum, the government's application seeks historical CSLI associated with [redacted] target cell phones for a period of sixty days, and that CSLI may be generated whenever a phone call is made or received, a text message is sent or received, or data is sent or received.

The cellular service providers for the [redacted] target cell phones are Verizon Wireless ("Verizon") and AT&T Wireless ("AT&T"). App. ¶ 1. The application also authorizes the government to obtain historical CSLI from any one of dozens of other cellular service providers (e.g., Cellular One, Sprint, and T-Mobile) that might have collected such information for any of the target cell phones. *Id.* ¶ 2. The application does so for two reasons. First, a provider other than Verizon or AT&T might have collected CSLI generated by one of the target cell phones if a

target user switched providers during the sixty-day period but kept the same phone number, a feature known as local number portability. *Id.* ¶ 2 n.2. Second, a provider other than Verizon or AT&T might have collected CSLI generated by one of the target cell phones if a target cell phone connected with the cell tower of that other provider over the course of the sixty-day period, an action known as "roaming." *See* ECF No. 26 Declaration of Public Defender Investigator Madeline Larsen ("Larsen Decl.") ¶ 2c. Roaming occurs when there is a gap in the network of a cell phone's provider and, as a result, the cell phone must connect to the cell tower of a different provider. *See id.* ¶¶ 2c, 4d (describing roaming on Verizon and AT&T networks).

Both Verizon and AT&T publish privacy policies telling their subscribers that location information is collected and may be turned over to the government. Verizon informs its subscribers, "We collect information about your use of our products, services and sites. Information such as . . . wireless location . . . ." Verizon, *Privacy Policy* (updated June 2015) ("Verizon Policy"), *available at* http://www.verizon.com/about/privacy/policy/. "We may," Verizon's policy continues, "disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as: to comply with valid legal process including subpoenas, court orders or search warrant." *Id.* In addition, the Verizon policy states: "Personally identifiable and other sensitive records are retained only as long as reasonably necessary for business, accounting, tax or legal purposes." *Id.*

AT&T, for its part, tells subscribers that it will collect their "location information," which includes "the whereabouts of your wireless device." AT&T, *Privacy Policy* (effective Sept. 16, 2013) ("AT&T Policy"), *available at* http://www.att.com/gen/privacy-policy?pid=2506. "Location information," says AT&T's policy, "is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies, including the satellites that comprise the Global Positioning System." *Id.* The AT&T policy states that AT&T "automatically collect[s] information" when the user uses AT&T's network, and that AT&T may provide this information to "government agencies" in order to "[c]omply with court orders." *Id.*

The policy also contains information concerning the accuracy of the "wireless location information" that AT&T collects and explains that AT&T "can locate your device based on the cell tower that's serving you" up to 1,000 meters in urban areas and 10,000 meters in rural areas. *Id.* Neither policy indicates how much location data Verizon or AT&T collects, nor does either policy estimate how long each provider will retain that information.

D. Procedural History

The government has submitted, under seal, an application for an order pursuant to 18 U.S.C. §§ 3122 and 3123 and 18 U.S.C. § 2703(d) seeking CSLI associated with [redacted] target cell phones. *See* ECF No. 2 at 1. The application sought historical CSLI for sixty days back from the date of the order, as well as prospective CSLI for sixty days going forward. *See id.* at 2. In support of its application to Judge Lloyd, the government submitted a letter brief on March 17, 2015. ECF No. 1.

On April 9, 2015, Judge Lloyd issued a public order denying the government's application. ECF No. 2. In that order, Judge Lloyd stated that he found "very persuasive" U.S. District Judge Susan Illston's analysis in *United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015), which held that the Fourth Amendment requires the government to secure a warrant supported by probable cause before obtaining sixty days' worth of historical CSLI. ECF No. 2 at 5. "[U]ntil binding authority says otherwise," Judge Lloyd concluded, "in order to get cell site information, prospective or historical, the government must obtain a search warrant under Rule 41 on a showing of probable cause." *Id.*

On April 30, 2015, the government appealed Judge Lloyd's order to the undersigned. Gov't Br. at 9. The government elected to appeal Judge Lloyd's denial of the application with respect to historical CSLI only. *See id.* at 1 ("The government appeals Judge Lloyd's Order to this Court to the extent Judge Lloyd denied the government historical cell site information."); *id.* at 3 n.1 ("As noted, however, the government is not appealing Judge Lloyd's order to the extent it denied the government prospective cell site information."). On May 7, 2015, the government filed

a supplemental brief regarding the Eleventh Circuit's en banc decision in *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015), which overruled the original panel opinion[2] cited by Judge Illston in *Cooper*. Gov't Supp. Br. at 3.

On May 20, 2015, the Court invited the Public Defender to file a written response to the arguments made in the government's appeal and supplemental brief. ECF No. 7. The Court also authorized the government to file a reply and set a hearing on the matter for June 24, 2015. *Id.* At a minimum, the requested briefing was to address "(1) whether the Supreme Court's decisions in *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), control the outcome here; (2) the Eleventh Circuit's en banc decision in *Davis*; and (3) whether if the Court concludes that the Fourth Amendment requires a warrant supported by probable cause, the Court must find any part of the Stored Communications Act unconstitutional." ECF No. 7 at 2. The Court also asked that the government be prepared to answer various questions regarding cell phone technology at the June 24 hearing. *Id.* at 2-3.

On June 12, 2015, the Public Defender filed its response to the government's appeal. ECF No. 17. Three days later, the Public Defender filed an amended response. Opp. at 32. On June 5, 2015, the Court granted separate requests by the ACLU and EFF to file amicus briefs in support of the Public Defender. ECF Nos. 12, 13. On June 12, 2015, the ACLU and EFF filed their amicus briefs. ACLU Br. at 18; EFF Br. at 13. On June 19, 2015, the government filed its reply. Gov't Reply at 12. The Court held a hearing on this matter on June 24, 2015.

On June 25, 2015, the Court ordered supplemental briefing on the issue of whether cellular service providers ever retain historical CSLI when that CSLI is generated from a cell phone's communications with the cell tower of another provider. ECF Nos. 24, 25. The government and

[2] The original panel opinion, authored by D.C. Circuit Judge David Bryan Sentelle sitting by designation, unanimously held that "cell site location information is within the subscriber's reasonable expectation of privacy" such that "[t]he obtaining of that data without a warrant is a Fourth Amendment violation." *United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015).

the Public Defender responded separately with filings on June 29, 2015. *See* Larsen Decl.; ECF No. 29-1, Declaration of Assistant U.S. Attorney Jeff Schenk ("Schenk Decl.").

II. LEGAL STANDARD

The Court reviews de novo a magistrate judge's legal conclusions and reviews any underlying factual findings for clear error. *See Quinn v. Robinson*, 783 F.2d 776, 811-12 (9th Cir. 1986); *accord United States v. McDermott*, 589 F. App'x 394, 395 (9th Cir. 2015). As Judge Lloyd's conclusion that the government must secure a search warrant on a showing of probable cause in order to obtain historical CSLI is a legal determination, this Court reviews that determination de novo.

III. DISCUSSION

A. Fourth Amendment Principles

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Cell phones plainly qualify as "effects" under the meaning of the Fourth Amendment. *See Oliver v. United States*, 466 U.S. 170, 177 n.7 (1984) ("The Framers would have understood the term 'effects' to be limited to personal, rather than real, property."). Further, as the text makes clear, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). "Where," as here, "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, reasonableness generally requires the obtaining of a judicial warrant." *Id.* (brackets omitted) (quoting *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995)). The Fourth Amendment's warrant requirement "ensures that the inferences to support a search are 'drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.'" *Id.* (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948). "In the absence of a warrant," the U.S. Supreme Court has held, "a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id.*

To determine whether a "search" has taken place such that the Fourth Amendment's warrant requirement is triggered, courts employ the reasonable expectation of privacy test established in *Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring).[3] Under *Katz*, the Court follows a "two-part inquiry." *California v. Ciraolo*, 476 U.S. 207, 211 (1986). First, the Court asks whether there exists a "subjective expectation of privacy in the object of the challenged search." *Kyllo v. United States*, 533 U.S. 27, 33 (2001). If so, the Court asks second whether "society [is] willing to recognize that expectation as reasonable." *Id.* (alteration in original). The Court now turns to this dual inquiry.

B. Fourth Amendment "Search"

1. Reasonable Expectation of Privacy in Historical CSLI

Neither the U.S. Supreme Court nor the Ninth Circuit has squarely addressed whether cell phone users possess a reasonable expectation of privacy in the CSLI, historical or otherwise, associated with their cell phones. The closest the Ninth Circuit has come was to issue a warning several years back in an unpublished decision: "The government's use at trial of [defendant's] cell site location information raises important and troublesome privacy questions not yet addressed by this court." *United States v. Reyes*, 435 F. App'x 596, 598 (9th Cir. 2011). In the absence of any binding authority, the Court ventures into this "troublesome" area of Fourth Amendment law as a matter of first impression.

Fortunately, the U.S. Supreme Court's cases on electronic surveillance prove instructive. In *United States v. Knotts*, the U.S. Supreme Court first applied the *Katz* test to electronic surveillance, holding that the Fourth Amendment was not violated when the government used a beeper to track a vehicle's movements on public roads. 460 U.S. 276, 277 (1983). The beeper

[3] A "search" also occurs for Fourth Amendment purposes "[w]hen the Government obtains information by physically intruding on persons, houses, papers, or effects." *Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) (internal quotation marks omitted). Here, there is no argument that the government's obtaining CSLI could constitute a search under this theory of common law trespass.

tracking in *Knotts* did not implicate the Fourth Amendment because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.* at 281. The *Knotts* Court, however, left open the possibility that advances in surveillance technology would require it to reevaluate its decision. *See id.* at 283-84 (explaining that "if such dragnet type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable").

The following year, in *United States v. Karo*, the U.S. Supreme Court cabined *Knotts* to surveillance in public places. 468 U.S. 705, 714 (1984). In *Karo*, the police placed a beeper in a container belonging to the defendant and monitored the beeper's location electronically, including while it was inside a private residence. *Id.* at 708-10. Tracking the beeper inside the home, the *Karo* Court explained, "reveal[ed] a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Id.* at 715. As a result, the *Karo* Court held that monitoring the beeper inside the home "violate[d] the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence," even though the officers could not have known, when they planted the tracking device, that it would end up inside a house. *Id.* at 714-15; *see also Kyllo*, 533 U.S. at 34 (holding that the government engages in a search in violation of the Fourth Amendment by using a thermal imager to detect heat signatures emanating from inside a house that would be invisible to the naked eye).

Most recently, in *United States v. Jones*, five Justices of the U.S. Supreme Court concluded that prolonged electronic location monitoring by the government, even when limited to public places, infringes on a legitimate expectation of privacy in violation of the Fourth Amendment. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring); *id.* at 965 (Alito, J., joined by Ginsburg, Breyer, & Kagan, JJ., concurring in the judgment). In *Jones*, the government installed a GPS tracking device on the defendant's car and used it to monitor the car's location—on public roads—

for twenty-eight days. *Id.* at 948 (majority opinion). The majority opinion held that the government violated the Fourth Amendment by the physical trespass of placing the tracking device on the vehicle without the defendant's consent. *Id.* at 949. The majority therefore did not need to address whether the government's location tracking also violated the defendant's reasonable expectation of privacy. *Id.* at 950-51. The majority explicitly noted, however, that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953.

The five Justices who did engage in a *Katz* analysis concluded that the government's actions in tracking the car's location over twenty-eight days violated the Fourth Amendment. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment). Although the government tracked the car only as it traveled in plain sight on public streets and highways, Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concluded that the GPS monitoring "involved a degree of intrusion that a reasonable person would not have anticipated." *Id.* at 964 (Alito, J., concurring in the judgment). Consequently, those four Justices found that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* Notably, this conclusion did not depend on the type of technology used to track the car in *Jones*. Rather, the four Justices emphasized the proliferation of modern devices that track people's movements, noting that cell phones were "perhaps [the] most significant" among these. *Id.* at 963.

Justice Sotomayor agreed with her four colleagues that prolonged electronic surveillance would violate the Fourth Amendment. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).[4] She added, however, that "even short-term monitoring" raises concerns under *Katz* because "GPS

[4] Justice Sotomayor also signed on to the majority's trespass-based holding. *Jones*, 132 S. Ct. at 954 (Sotomayor, J., concurring) ("I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, where, as here, the Government obtains information by physically intruding on a constitutionally protected area." (brackets and internal quotation marks omitted)).

monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* Justice Sotomayor was particularly concerned with "the existence of a reasonable societal expectation of privacy in *the sum* of one's public movements." *Id.* at 956 (emphasis added). In particular, she wondered "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Id.*; *see also CIA v. Sims*, 471 U.S. 159, 178 (1985) (finding it within the CIA director's discretion not to disclose "superficially innocuous information" that might reveal an intelligence source's identity because "what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context" (brackets and internal quotation marks omitted)). When governmental actions intrude upon someone's privacy to that degree, Justice Sotomayor concluded, a warrant is required. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

Two years later, the U.S. Supreme Court cited Justice Sotomayor's concurrence in *Jones* with approval in holding that police must obtain a warrant to search the contents of an arrestee's cell phone. *Riley v. California*, 134 S. Ct. 2473, 2490 (2014). Prior to *Riley*, the U.S. Supreme Court had adopted a categorical rule that, under the longstanding search-incident-to-arrest exception to the warrant requirement, the police need not obtain a warrant before searching "personal property immediately associated with the person of the arrestee." *Id.* at 2484 (ellipsis omitted) (quoting *United States v. Chadwick*, 433 U.S. 1, 15 (1977)); *see also United States v. Robinson*, 414 U.S. 218, 235 (1973). In holding that a warrant was required to search the contents of an arrestee's cell phone, the *Riley* Court found that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person." 134 S. Ct. at 2489. In addition to "their immense storage capacity" and "pervasiveness" in American society, cell phones were further distinguished from conventional items an arrestee might be carrying in

that "[d]ata on a cell phone can also reveal where a person has been." *Id.* at 2489-90. Relying on Justice Sotomayor's concurrence in *Jones*, the *Riley* Court explained its concern: "Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Id.* at 2490.

Based on the preceding U.S. Supreme Court cases, the following principles are manifest: (1) an individual's expectation of privacy is at its pinnacle when government surveillance intrudes on the home; (2) long-term electronic surveillance by the government implicates an individual's expectation of privacy; and (3) location data generated by cell phones, which are ubiquitous in this day and age, can reveal a wealth of private information about an individual. Applying those principles to the information sought here by the government, the Court finds that individuals have an expectation of privacy in the historical CSLI associated with their cell phones, and that such an expectation is one that society is willing to recognize as reasonable. *See Katz*, 389 U.S. at 360-61 (Harlan, J., concurring).

Here, as in *Jones*, the government seeks permission to track the movement of individuals—without a warrant—over an extended period of time and by electronic means. CSLI, like GPS, can provide the government with a "comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Riley*, 134 S. Ct. at 2490 (quoting *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)). With the proliferation of smaller and smaller base stations such as microcells, picocells, and femtocells—which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home, *see* Blaze Testimony at 43-44—the government is able to use historical CSLI to track an individual's past whereabouts with ever increasing precision. *See Riley*, 134 S. Ct. at 2490 (explaining that a cell phone's "[h]istoric location information . . . can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building"). At oral argument, the government agreed that

in some instances CSLI could locate an individual within her home, Hr'g Tr. at 30:15-20, 31:16-32:4, and did not dispute that CSLI will become more precise as the number of cell towers continues to multiply, *id.* at 32:5-9. This admission is of constitutional significance because rules adopted under the Fourth Amendment "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36.

In fact, the information the government seeks here is arguably more invasive of an individual's expectation of privacy than the GPS device attached to the defendant's car in *Jones*. This is so for two reasons. First, as the government conceded at the hearing, over the course of sixty days an individual will invariably enter constitutionally protected areas, such as private residences. Hr'g Tr. at 18:15-24. Tracking a person's movements inside the home matters for Fourth Amendment purposes because "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Karo*, 468 U.S. at 714; *see also Kyllo*, 533 U.S. at 31 ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." (internal quotation marks omitted)). As one court put it, "Because cellular telephone users tend to keep their phone on their person or very close by, placing a particular cellular telephone within a home is essentially the corollary of locating the user within the home." *See In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 849 F. Supp. 2d 526, 541 (D. Md. 2011).

Second, the government conceded at oral argument that, compared to GPS tracking of a car, the government will "get more information, more data points, on the cell phone" via historical CSLI. Hr'g Tr. at 29:8-9; *see also id.* at 29:19-21 ("But, yes, of course the person has the phone more than they have their car, most people at least do, so it gives [the government] more data."). Cell phones generate far more location data because, unlike the vehicle in *Jones*, cell phones typically accompany the user wherever she goes. *See* Wessler Decl. ¶¶ 8-10 (describing a Sixth

Circuit case, *United States v. Carpenter*, where the government obtained 23,034 cell site location data points for one defendant over a period of eighty-eight days). Indeed, according to a survey cited by the U.S. Supreme Court in *Riley*, "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." 134 S. Ct. at 2490 (citing Harris Interactive, *2013 Mobile Consumer Habits Study* (June 2013)).

In finding a reasonable expectation of privacy in historical CSLI, the Court notes its agreement with another judge in this district. In *United States v. Cooper*, No. 13-CR-00693-SI-1, 2015 WL 881578, at *8 (N.D. Cal. Mar. 2, 2015), Judge Illston observed that "many, if not most, will find their cell phone quite literally attached to their hip throughout the day." "All the while," Judge Illston continued, "these phones connect to cell towers, and thereby transmit enormous amounts of data, detailing the phone-owner's physical location any time he or she places or receives a call or text." *Id.* "However, there is no indication to the user that making [a] call will also locate the [user]." *Id.* (internal quotation marks omitted) (quoting *Third Circuit Opinion*, 620 F.3d at 317). This Court agrees further with Judge Illston that an individual's "reasonable expectation of privacy in his or her location is especially acute when the call is made from a constitutionally protected area, such as inside a home." *Id.* Judge Illston's reasoning is all the more compelling when one considers that historical CSLI is also generated by passive activities such as automatic pinging, continuously running applications ("apps"), and the receipt of calls and text messages. Moreover, over a sixty-day period, as the government concedes, the government would inevitably obtain CSLI generated from inside the home. Hr'g Tr. at 18:15-24.

Furthermore, the Public Defender and amici point to evidence that individuals harbor a subjective expectation of privacy in the historical CSLI associated with their cell phones. For example, EFF informs the Court that in a 2014 survey, the Pew Research Center ("Pew") found that 82% of American adults consider details of their physical location over time to be sensitive information. EFF Br. at 2 (citing Pew Research Ctr., *Public Perceptions of Privacy and Security*

in the Post-Snowden Era 32 (2014), *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf). This figure is higher than the percentage of individuals surveyed who consider their relationship history, religious or political views, or the content of their text messages to be sensitive. *Id.* at 2-3. In a 2012 survey, Pew found that smartphone owners typically take precautions to protect access to their mobile data, with nearly one-third of them responding that they had turned off the location tracking feature on their phone due to concerns over who might access that information. *See* Jan Lauren Boyles et al., Pew Research Internet & Am. Life Project, *Privacy and Data Management on Mobile Devices* 3-4, 8 (2012), *available at* http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Mobile PrivacyManagement.pdf. Further, a 2013 survey conducted on behalf of the Internet company TRUSTe found that 69% of American smart phone users did not like the idea of being tracked. David Deasy, *TRUSTe Study Reveals Smartphone Users More Concerned About Mobile Privacy Than Brand or Screen Size*, TRUSTe Blog (Sept. 5, 2013), http://www.truste.com/blog/2013/09/05/truste-study-reveals-smartphone-users-more-concerned-about-mobile-privacy-than-brand-or-screen-size/. The government does not dispute this evidence, which the Court properly considers. *See Riley*, 134 S. Ct. at 2490 (relying on survey data demonstrating the ubiquity of cell phones).

This survey data is all the more salient because cell phone users who take affirmative measures to protect their location information may still generate CSLI that the government can obtain. EFF cites Pew surveys from 2012 showing that 30% of all smart phone owners turned off location tracking on their phones while "46% of teenagers turned location services off." EFF Br. at 3. Turning off location services, however, does not preclude CSLI from being generated. As the ACLU explains, "many smartphones include a location privacy setting that, when enabled, prevents applications from accessing the phone's location. But this setting has no impact upon carriers' ability to learn the cell sector in use." ACLU Br. at 13. In other words, even though a user may demonstrate a subjective expectation of privacy by disabling an app's location

identification features, that user's cell phone will still generate CSLI whenever the phone makes or receives a call, sends or receives a text, sends or receives data, or merely "checks in" with a nearby cell tower.

What is more, society's expectation of privacy in historical CSLI is evidenced by the myriad state statutes and cases suggesting that cell phone users "can claim a justifiable, a reasonable, or a legitimate expectation of privacy" in this kind of information. *Knotts*, 460 U.S. at 280 (internal quotation marks omitted). Although state law is not dispositive of the issue, "the recognition of a privacy right by numerous states may provide insight into broad societal expectations of privacy." *Cooper*, 2015 WL 881578, at *8 (quoting *United States v. Velasquez*, No. CR 08-0730 WHA, 2010 WL 4286276, at *5 (N.D. Cal. Oct. 22, 2010)). In California, for instance, where this Court sits, it has been the law for more than three decades that police need a warrant to obtain telephone records. *See People v. Blair*, 25 Cal. 3d 640, 654-55 (1979); *see also People v. Chapman*, 36 Cal. 3d 98, 107 (1984) ("This court held [in *Blair*] that under the California Constitution, [telephone] records are protected from warrantless disclosure."), *disapproved of on other grounds by People v. Palmer*, 24 Cal. 4th 856 (2001). As *Blair* involved nothing more than "a list of telephone calls" made from the defendant's California hotel room, *see Blair*, 25 Cal. 3d at 653, there is little doubt that the California Supreme Court's holding applies with full force to the government's application here, which seeks historical CSLI generated by a target cell phone's every call, text, or data connection, in addition to any telephone numbers dialed or texted.

Outside of California, the high courts of Florida, Massachusetts and New Jersey have all recognized a reasonable expectation of privacy in CSLI. *See Tracey v. State*, 152 So. 3d 504, 525-26 (Fla. 2014) (prospective CSLI); *Commonwealth v. Augustine*, 4 N.E.3d 846, 850 (Mass. 2014) (historical CSLI); *State v. Earls*, 70 A.3d 630, 644 (N.J. 2013) (prospective CSLI). The high courts of Massachusetts and New Jersey found a reasonable expectation of privacy under their respective state constitutions, while the Florida Supreme Court based its ruling on the federal

Fourth Amendment. In reaching its decision, the Florida Supreme Court explained that "because cell phones are indispensable to so many people and are normally carried on one's person, cell phone tracking can easily invade the right to privacy in one's home or other private areas, a matter that the government cannot always anticipate and one which, when it occurs, is clearly a Fourth Amendment violation." *Tracey*, 152 So. 3d at 524. Relying on Justice Sotomayor's concurrence in *Jones*, the Florida Supreme Court found that "owners of cell phones or cars equipped with GPS capability do not contemplate that the devices will be used to enable covert surveillance of their movements." *Id.* (citing *Jones*, 132 S. Ct. at 956 at n.* (Sotomayor, J., concurring)). On that basis, the *Tracey* Court held that the defendant "had a subjective expectation of privacy in the location signals transmitted solely to enable the private and personal use of his cell phone," and that "such a subjective expectation of privacy of location as signaled by one's cell phone—even on public roads—is an expectation of privacy that society is now prepared to recognize as objectively reasonable." *Id.* at 525-26 (citing *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring)).

Six more states have legislated privacy protections for historical CSLI. Colorado, Maine, Minnesota, Montana, Tennessee, and Utah have passed statutes expressly requiring law enforcement to apply for a search warrant to obtain this data. *See* Colo. Rev. Stat. § 16-3-303.5(2); Me. Rev. Stat. tit. 16, § 648; Minn. Stat. §§ 626A.28(3)(d), 626A.42(2); Mont. Code Ann. § 46-5-110(1)(a); Tenn. Code Ann. § 39-13-610(b); Utah Code Ann. § 77-23c-102(1)(a). In Utah, for example, "a government entity may not obtain the location information . . . of an electronic device without a search warrant issued by a court upon probable cause," subject to a handful of exceptions. Utah Code Ann. § 77-23c-102(1)(a). At least six additional states—Illinois, Indiana, Maryland, Virginia, Washington, and Wisconsin—have passed laws requiring police to obtain a search warrant to track a cell phone in real time. *See* 725 Ill. Comp. Stat. 168/10; Ind. Code § 35-33-5-12; Md. Code Ann., Crim. Proc. § 1-203.1; Va. Code Ann. 19.2-56.2; Wash. Rev. Code 9.73.260; Wis. Stat. § 968.373(2). Indiana, for instance, generally bars government tracking of cell phones in real time unless law enforcement "has obtained an order

issued by a court based upon a finding of probable cause to use the tracking instrument." Ind. Code § 35-33-5-12(a).

For all the foregoing reasons, the Court concludes that cell phone users have an expectation of privacy in the historical CSLI associated with their cell phones, and that society is prepared to recognize that expectation as objectively reasonable. Cell phone users do not expect that law enforcement will be able to track their movements 24/7 for a sixty-day period simply because the users keep their cell phones turned on. That expectation, the Court finds, is eminently reasonable.

2. Third-Party Doctrine

The Court now addresses whether the so-called "third-party doctrine" destroys cell phone users' reasonable expectation of privacy in the historical CSLI associated with their cell phones. The government argues that the third-party doctrine established by the U.S. Supreme Court in cases like *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), deprives cell phone users of any reasonable expectation of privacy in their historical CSLI. *See* Gov't Br. at 3-6; Gov't Reply at 4-8. Under *Miller* and *Smith*, the government contends, "the Supreme Court has squarely held that individuals have no expectation of privacy in information that they voluntarily share with third parties, and that principle forecloses any claim that individuals have a reasonable expectation of privacy in historical cell site information." Gov't Reply at 4. For the reasons stated below, the Court disagrees.

a. Passive Generation of Historical CSLI by Continually Running Apps and Automatic Pinging Renders *Miller* and *Smith* Inapposite

As *Miller* and *Smith* make clear, the third-party doctrine applies when an individual has "voluntarily conveyed" to a third party the information that the government later obtains. In 1976, the U.S. Supreme Court in *Miller* held that an individual making a deposit at a bank had no expectation of privacy in records of transactions that were held by the bank. 425 U.S. at 437. In arriving at this conclusion, the *Miller* Court focused on whether the bank records at issue implicated a reasonable expectation of privacy: "We must examine the nature of the particular

documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Id.* at 442 (quoting *Couch v. United States*, 409 U.S. 322, 335 (1973)). The *Miller* Court's ultimate conclusion—that the defendant had no such expectation—turned not on the fact that the records were owned or possessed by the bank, but on the fact that the defendant had "voluntarily conveyed" the information contained therein to the bank and its employees. *Id.* To that end, the *Miller* Court 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." *Id.* at 443.

Three years later, in 1979, the U.S. Supreme Court in *Smith* held that the government's use of a pen register over a period of three days to capture the numbers dialed from a home landline telephone was not a search under the Fourth Amendment. 442 U.S. at 737, 742. The *Smith* Court found that telephone users do not maintain a subjective expectation of privacy in the numbers they dial 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." *Id.* at 742. The *Smith* Court, citing *Miller*, also found no objectively reasonable expectation of privacy in dialed telephone numbers, reiterating "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. "When he used his phone," the *Miller* Court explained, "petitioner voluntarily conveyed numerical information to the telephone company," destroying his reasonable expectation of privacy in that information. *Id.* at 744.

Cell phone users, by contrast, do not "voluntarily convey" their location to the cellular service provider in the manner contemplated by *Miller* and *Smith*. This is especially true when historical CSLI is generated just because the cell phone is on, such as when cell phone apps are sending and receiving data in the background or when the cell phone is "pinging" a nearby cell

tower. As the government's FBI special agent explained, "CSLI for a cellular telephone may still be generated in the absence of user interaction with a cellular telephone." Luna Decl. ¶ 3B. "For example," the special agent continued, CSLI may be generated by "applications that continually run in the background that send and receive data (e.g. email applications)." *Id.* At oral argument, the government confirmed that its § 2703(d) application authorizes the government to obtain historical CSLI generated by such activities. *See* Hr'g Tr. at 51:4-5.

In addition, the government's FBI special agent informed the Court that a cell phone "is always scanning its network's cellular environment." Luna Decl. ¶ 3B. In so doing, a cell phone periodically identifies itself to the closest cell tower—not necessarily the closest cell tower geographically, but the one with the strongest radio signal—as it moves through its network's coverage area. *Id.*; Blaze Testimony at 50. This process, known as "registration" or "pinging," facilitates the making and receiving of calls, the sending and receiving of text messages, and the sending and receiving of cell phone data. *See id.* Pinging nearby cell towers is automatic and occurs whenever the phone is on, without the user's input or control. DHS Lesson Plan at 9. This sort of pinging happens every seven to nine minutes. *Id.* When "investigators desire to map the physical movement of a subject" through historical CSLI, they may do so by obtaining "[a] record of subject phone pings" from cellular service providers. *Id.* at 10. It is not clear that every cellular service provider records CSLI generated by such pings, *see id.*, but the Court was informed at oral argument that Sprint, one of the cellular service providers listed in the government's application, does so, *see* Hr'g Tr. at 4:19-5:6. Although Sprint is not the service provider for any of the target cell phones, the government concedes that the instant application allows the government to obtain historical CSLI from Sprint if the target cell phones were to roam onto Sprint's network[5] or if one of the targets were to switch from Verizon or AT&T to Sprint during the sixty-day period but keep the same phone number pursuant to local number portability. *See* Schenk Decl. ¶ 1a; App. ¶ 2 &

[5] Verizon and Sprint utilize "the same kind of system; so Sprint phones can connect to Verizon towers and vice versa." Larsen Decl. ¶ 3a.

n.2.

In *Miller* and *Smith*, the individual knew with certainty the information that was being conveyed and the third party to which the conveyance was made. Cell phone users, on the other hand, enjoy far less certainty with respect to CSLI. CSLI, in contrast to deposit slips or digits on a telephone, is neither tangible nor visible to a cell phone user. When the telephone user in *Smith* received his monthly bill from the phone company, the numbers he dialed would appear. *See* 442 U.S. at 742. The CSLI generated by a user's cell phone makes no such appearance. *See* Larsen Decl. ¶ 3c. Rather, because CSLI is generated automatically whenever a cell tower detects radio waves from a cell phone, a cell phone user typically does not know that her phone is communicating with a cell tower, much less the specific cell tower with which her phone is communicating. *See* Hr'g Tr. at 16:7-9. It may be, as the government explained, that a cell phone connects to "many towers" during the length of a call, *id.* at 3:9, and the tower to which a cell phone connects is not necessarily the closest one geographically, *id.* at 31:21-22. Moreover, when an app on the user's phone is continually running in the background, *see* Luna Decl. ¶ 3B, she may not be aware that the cell phone in her pocket is generating CSLI in the first place.

Roaming poses an additional problem. As stated previously, roaming occurs when there is a gap in the network of a cell phone's provider and, as a result, the cell phone must connect to the cell tower of a different provider. *See* Larsen Decl. ¶¶ 2c, 4d (discussing roaming). Typically, a cell phone user does not know when her phone is roaming onto another provider's network, much less the name of the other provider on whose network her phone is roaming. As a result, cell phone users, unlike a bank depositor or telephone dialer, will often not know the identity of the third party to which they are supposedly conveying information. Unlike her counterparts in *Miller* or *Smith*, a cell phone user therefore has less reason to suspect that she is disclosing information to a third party, especially since she may not even know that the information is being disclosed or who the third party is.

In light of the foregoing, the Court concludes that historical CSLI generated via

continuously operating apps or automatic pinging does not amount to a *voluntary* conveyance of the user's location twenty-four hours a day for sixty days. Such data, it is clear, may be generated with far less intent, awareness, or affirmative conduct on the part of the user than what was at issue in *Miller* and *Smith*. Unlike the depositor in *Miller* who affirmatively conveyed checks and deposit slips to the bank, or the telephone user in *Smith* who affirmatively dialed the numbers recorded by the pen register, a cell phone user may generate historical CSLI simply because her phone is on and without committing any affirmative act or knowledge that CSLI is being generated. *Smith*, for example, never contemplated the disclosure of information while the landline telephone was not even in use.

This sort of passive generation of CSLI does not amount to a voluntary conveyance under the third-party doctrine. The Ninth Circuit has distinguished information "passively conveyed through third party equipment" from information "voluntarily turned over" to a third party, the latter of which is governed by the third-party doctrine. *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). In the same vein, the Sixth Circuit found *Smith* distinguishable where federal law enforcement had dialed the defendant's cell phone without allowing it to ring and used the resulting CSLI to track his movements. *United States v. Forest*, 355 F.3d 942, 947 (6th Cir. 2004), *judgment vacated on other grounds sub nom. Garner v. United States*, 543 U.S. 1100 (2005). In that instance, the Sixth Circuit agreed, the defendant "did not voluntarily convey his cell site data to anyone." *Id.* (internal quotation marks omitted).

Other courts have taken a similar view. The Third Circuit, for example, rejected the government's argument that *Miller* and *Smith* precluded magistrate judges from requiring a warrant supported by probable cause to obtain historical CSLI. *Third Circuit Opinion*, 620 F.3d at 317-18. "A cell phone customer," the Third Circuit explained, "has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[6] *Id.* at 317. Likewise, the

[6] In finding that cell phone users do not voluntarily convey historical CSLI to cellular service providers, the Third Circuit agreed with the opinion of U.S. Magistrate Judge Lisa Pupo Lenihan, the Magistrate Judge below. *See In re U.S. for an Order Directing a Provider of Elec.*

Florida Supreme Court, citing the Third Circuit's opinion, concluded that the third-party doctrine did not control: "Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes, and which enable cell phone applications to operate for navigation, weather reporting, and other purposes, does not mean that the user is consenting to use of that location information by third parties for any other unrelated purposes." *Tracey*, 152 So. 3d at 522. One court, moreover, found it "difficult to understand how the user 'voluntarily' expose[s] [CSLI] to a third party" where the government seeks "information—essentially, continuous pinging—that is not collected as a necessary part of cellular phone service, nor generated by the customer in placing or receiving a call." *In re Application*, 849 F. Supp. 2d at 539 n.6.

Furthermore, the mere fact that historical CSLI is a record maintained by a cellular service provider, and not kept by the user, does not defeat the user's expectation of privacy in what that information reveals—namely, the user's location at any moment her cell phone communicates with a cell tower. As the Ninth Circuit has explained, "it is clear that neither ownership nor possession is a necessary or sufficient determinant of the legitimacy of one's expectation of privacy." *DeMassa v. Nunez*, 770 F.2d 1505, 1507 (9th Cir. 1985).

Indeed, in *Ferguson v. City of Charleston*, 532 U.S. 67, 76-78 (2001), the U.S. Supreme Court held that law enforcement needed a warrant to obtain drug testing results from the urine of pregnant women, even though the results were kept by a third party state hospital. The *Ferguson* Court so held because "[t]he reasonable expectation of privacy enjoyed by the typical patient

---

Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 615 (W.D. Pa. 2008) (concluding that "CSLI is not 'voluntarily and knowingly' conveyed by cell phone users"), *vacated on other grounds sub nom. Third Circuit Opinion*, 620 F.3d 304 (3d Cir. 2010). Judge Lenihan's opinion was notable, the Third Circuit explained, because it "was joined by the other magistrate judges in that district." *Third Circuit Opinion*, 620 F.3d at 308. The Third Circuit continued: "This is unique in the author's experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan's opinion has among her colleagues who, after all, routinely issue warrants authorizing searches and production of documents." *Id.*

undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[7] *Id.* at 78. Similarly, here, a cell phone user's reasonable expectation of privacy in her location at virtually all times is not destroyed simply because law enforcement would have to obtain the records of her whereabouts from a third party. *See United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (finding a reasonable expectation of privacy in the content of e-mails stored by a third-party service provider); *cf. United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (recognizing "a legitimate expectation of privacy" in "[l]etters and other sealed packages" even though they may be entrusted to third-party mail carriers while in transit); *Stoner v. California*, 376 U.S. 483, 487-88, 490 (1964) (rejecting the argument that "the search of [a] hotel room, although conducted without the petitioner's consent, was lawful because it was conducted with the consent of the hotel clerk," because a hotel guest's Fourth Amendment rights cannot be "left to depend on the unfettered discretion" of a third party clerk).

Importantly, the Court is not holding that *Miller* and *Smith* are no longer good law. Only the U.S. Supreme Court may do so.[8] The Court instead finds that *Miller* and *Smith* do not control the analysis here because the generation of historical CSLI via continually running apps or routine pinging is not a voluntary conveyance by the cell phone user in the way those cases demand. Where, as here, an individual has not voluntarily conveyed information to a third party, her expectation of privacy in that information is not defeated under the third-party doctrine. *See, e.g.*, *Third Circuit Opinion*, 620 F.3d at 317-18; *Tracey*, 152 So. 3d at 522.

[7] The *Ferguson* majority made no mention of the third-party doctrine, an omission underscored by Justice Scalia in dissent. 532 U.S. at 94-95 (Scalia, J., dissenting).

[8] The Court notes that in her concurrence in *Jones*, Justice Sotomayor wrote that *Miller* and *Smith*, two cases decided in the 1970s, were "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." 132 S. Ct. at 957 (Sotomayor, J., concurring).

b. The Factual Record Before the Fifth and Eleventh Circuits Did Not Include Continually Running Apps and Automatic Pinging

This conclusion is not at odds with the decisions of the Fifth and Eleventh Circuits because the factual record in those cases was materially different. Both cases involved technology from 2010 and were expressly limited to instances where a cell phone user was either making or receiving a call. The Fifth Circuit, for example, held that *Smith* controlled the analysis because a cell phone user "understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call," and therefore "voluntarily conveys his cell site data each time he makes a call." *Fifth Circuit Opinion*, 724 F.3d at 612-14.

Similarly, the Eleventh Circuit en banc held that the "longstanding third-party doctrine plainly controls the disposition of this case" because "[c]ell phone users voluntarily convey cell tower location information to telephone companies in the course of making and receiving calls on their cell phones." *Davis*, 785 F.3d at 512 & n.12. "Just as in *Smith*," the Eleventh Circuit continued, "users could not complete their calls without necessarily exposing this information to the equipment of third-party service providers." *Id.* at 512 n.12.

Neither circuit, however, had occasion to address whether a cell phone user voluntarily conveys her location to a cellular service provider when the historical CSLI is generated by continuously operating apps or automatic pinging. The Fifth Circuit's decision only contemplated instances where the cell phone user "makes a call." *Fifth Circuit Opinion*, 724 F.3d at 614. The Fifth Circuit may have limited its analysis in this way because, according to the government there, "cell phone service providers do not create cell site records when a phone is in an idle state." *Id.* at 602 n.1. This is contrary to the factual record here, which indicates that "CSLI for a cellular telephone may still be generated in the absence of user interaction with a cellular telephone." Luna Decl. ¶ 3B. "For example," the government's FBI special agent explained, "CSLI may still be generated" by "applications that continually run in the background that send and receive data (e.g. email applications)." *Id.*

The Fifth Circuit's analysis may also have been so limited because the government's

application for historical CSLI was filed in 2010. *Fifth Circuit Opinion*, 724 F.3d at 602. In fact, before the Fifth Circuit, the government argued that CSLI was "not sufficiently accurate to reveal when someone is in a private location such as a home." *Id.* at 609. Here, by contrast, the government explained at oral argument that CSLI from a femtocell could be used to locate an individual at her home. Hr'g Tr. at 31:16-32:4. This distinction has constitutional significance because femtocells, like the beeper in *Karo*, can "reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant."[9] 468 U.S. at 715.

The Eleventh Circuit's decision was equally limited by its facts. The en banc panel in *Davis* cabined its voluntariness analysis to making or receiving phone calls because the cellular provider at issue there did not record "any cell tower location information for when the cell phone was turned on but not being used to make or receive a call."[10] 785 F.3d at 503. Judge Adalberto Jordan emphasized this point in his concurrence: "Finally, it is important to reiterate that the cell site information was generated from calls Mr. Davis made and received on his cellphone, and was not the result of his merely having his cellphone turned on. There was, in other words, no passive tracking based on Mr. Davis' mere possession of a cellphone, and I do not read the Court's opinion as addressing such a situation." *Id.* at 524 (Jordan, J., concurring).

---

[9] That *Smith* involved a home landline telephone is of no moment. Regardless of the petitioner's location, the *Smith* Court found, "his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." 442 U.S. at 743. When, as in this case, the information the government seeks is an individual's location, the U.S. Supreme Court's subsequent case law on electronic surveillance is more on point. *See, e.g.*, *Karo*, 468 U.S. at 714 (emphasizing that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable").

[10] The cellular service provider in *Davis* also did not record "any data at all for text messages sent or received." 785 F.3d at 503. This fact did not go unnoticed by the dissent, which explained that "the vast majority of communications from cell phones are in the form of text messages and data transfers, not phone calls." *Id.* at 542 (Martin, J., dissenting). "The frequency of text messaging," continued the dissent, "is much greater than the frequency of phone calling—particularly among young cell phone users." *Id.* The Fifth Circuit's decision also did not address text messaging.

Further, the Eleventh Circuit, just like the Fifth Circuit, "limit[ed] its decision to the world (and technology) as we knew it in 2010." *Davis*, 785 F.3d at 521 (Jordan, J., concurring); *see also id.* at 502 (majority opinion) (explaining that the government sought historical CSLI "for the period from August 1, 2010 through October 6, 2010). Indeed, the court in *Davis* expressly declined to consider "newer technology," such as "femtocells," that had developed since 2010. *Id.* at 503 n.7 (majority opinion). This Court, in contrast, must consider the state of the technology as it exists in June 2015 as well as going forward. *See Kyllo*, 533 U.S. at 35-36 (rejecting "a mechanical interpretation of the Fourth Amendment" because courts "must take account of more sophisticated systems that are already in use or in development"). That technology includes femtocells, which the government says can be used to locate an individual within her home. *See* Hr'g Tr. at 29:22-33:25 (government discussion of femtocell technology).

It is clear, then, that the factual record before this Court is distinct. It is not the case here that "the signal [to a cell tower] *only* happens when a user makes or receives a call." *Davis*, 785 F.3d at 498 (emphasis added). Rather, historical CSLI is also generated by continuously operating apps and by frequent pinging. Luna Decl. ¶ 3B. Critically, the government here does not disclaim its purported right to obtain without a warrant historical CSLI generated by such passive activities. This is true even though, as explained above, the government's application "does not seek" CSLI "that might be available when the [target cell phones] are turned 'on' but a call is not in progress." App. ¶ 3. Because the government broadly defines "call" to include any call, text message, or data transfer, *see* Hr'g Tr. at 50:22-52:5, the government's application could very well obtain historical CSLI generated by "applications that continually run in the background that send and receive data," Luna Decl. ¶ 3B.

Nor is it the case here that "[u]sers are aware that cell phones do not work when they are outside the range of *the* provider company's cell tower network." *Davis*, 785 F.3d at 511 (emphasis added). Whatever the factual record may have been before the Fifth and Eleventh Circuits, the record here establishes that a user's cell phone works—and generates CSLI—when

the user is outside the range of her provider's cell tower network but roams onto the network of another provider. *See* Larsen Decl. ¶¶ 2c, 4d (describing roaming on Verizon and AT&T networks). It is only when a cell phone cannot connect to the network of *any* provider that the cell phone will not generate CSLI. Neither the Fifth Circuit nor the Eleventh Circuit addressed roaming or considered whether roaming impacts the voluntary conveyance analysis.

These twin factual distinctions—(1) that historical CSLI may be generated by continually running apps and automatic pinging; and (2) that historical CSLI may be recorded and turned over to the government by any number of cellular service providers other than the cell phone user's—are essential to the Court's finding of no voluntary conveyance. As the Fifth Circuit and the Eleventh Circuit had no occasion to consider them, those decisions do not undermine the Court's conclusion that the third-party doctrine does not govern the facts here.

c. Passive Receipt of Calls and Texts Is Not A Voluntary Conveyance Either

The Court has established that the generation of historical CSLI via continually running apps or routine pinging is not a voluntary conveyance by the cell phone user in the way *Miller* and *Smith* demand. This showing, on its own, is sufficient for the Court to conclude that the third-party doctrine does not defeat a cell phone user's reasonable expectation of privacy in the historical CSLI associated with her cell phone.

Nonetheless, the Court also finds that the passive receipt of calls and text messages does not amount to a voluntary conveyance under the meaning of *Miller* and *Smith*. In *Miller*, the bank patron affirmatively conveyed checks and deposit slips to the bank. 425 U.S. at 437. In *Smith*, the telephone user affirmatively dialed the numbers recorded by the pen register. 442 U.S. at 737, 742. Here, by contrast, a cell phone user who receives an unwanted or unanswered call or an unwanted text generates historical CSLI without the commission of any similar affirmative act. As the government's FBI special agent explained, "CSLI for a cellular telephone may still be generated in the absence of user interaction with a cellular telephone." Luna Decl. ¶ 3B. As one example, the special agent stated that "CSLI may still be generated during an incoming voice call

that is not answered." *Id.* When an unanswered call goes to voicemail, it may be hours before the cell phone user even realizes that she has been called. The historical CSLI, however, will generate as soon as that call was received.

At the hearing the government appeared to recognize that generation of CSLI via passive receipt of calls or texts involves less affirmative conduct than what was at issue in *Miller* and *Smith*: "It certainly feels like it's a different affirmative act by the person holding the phone if they can be called and, as a result, all this data is created, as opposed to them making the affirmative act of calling." Hr'g Tr. at 39:16-19. The government agreed with the Court, moreover, that "there's nothing to prevent . . . the creation, potentially, of cell site information by the government if [the government] really wanted to know where someone was at a given moment." *Id.* at 55:7-9. As the government acknowledged, "We all know how to create cell site location information." *Id.* at 55:11-12. Such a "ruse," as the government calls it, *id.* at 55:14, is far from fantasy. In *Forest*, for example, the Sixth Circuit found *Smith* distinguishable where federal law enforcement repeatedly dialed the defendant's cell phone and used the resulting CSLI to track his whereabouts. 355 F.3d at 947. In that case, the Sixth Circuit found that the defendant's receipt of government calls was not voluntary. *Id.*

The Third Circuit, in finding that *Miller* and *Smith* did not foreclose magistrate judges from demanding a warrant supported by probable cause to obtain historical CSLI, concluded likewise that mere receipt of phone calls is not a voluntary conveyance:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, 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*.

Third Circuit Opinion, 620 F.3d at 317-18 (emphasis added) (brackets and internal quotation marks omitted). It is one thing to say that cell phone users voluntarily convey the numbers they

dial to the cellular service provider so that a call may be connected. *Smith*, though involving a home landline telephone, says as much. From that premise, however, it does not follow that cell phone users also voluntarily convey their *location* merely by possessing a cell phone that is capable of receiving calls and texts without warning and at any time of day. Other district courts have taken the same view. *See, e.g.*, *Cooper*, 2015 WL 881578, at *8 (agreeing with the Third Circuit that "when a cell phone user receives a call, he hasn't voluntarily exposed anything at all" (internal quotation marks omitted)).

The Fifth Circuit did not directly address receipt of phone calls, despite quoting from the Third Circuit's opinion. *See Fifth Circuit Opinion*, 724 F.3d at 613-14 (discussing voluntary conveyance when a cell phone user "makes a call" only). For its part, the Eleventh Circuit opted to combine making and receiving calls in its analysis. *See Davis*, 785 F.3d at 512 n.12 ("Cell phone users voluntarily convey cell tower location information to telephone companies in the course of *making and receiving* calls on their cell phones. Just as in *Smith*, users could not complete their calls without necessarily exposing this information to the equipment of third-party service providers." (emphasis added)). Neither opinion, as indicated above, addressed receipt of text messages. *See supra* note 10.

For the reasons stated above, the Court finds that the Third Circuit has the better of the argument: "when a cell phone user receives a call [or text], he hasn't voluntarily exposed anything at all." *Third Circuit Opinion*, 620 F.3d at 317-18 (internal quotation marks omitted). Unlike the bank depositor in *Miller* or the telephone dialer in *Smith*, a cell phone user receiving an unanswered call or an unsolicited text has committed no affirmative act. She has done nothing more than leave her phone on.

Accordingly, the Court finds that *Miller* and *Smith* do not control the analysis here for the additional reason that the generation of historical CSLI via passive receipt of phone calls and text messages is not a voluntary conveyance by the cell phone user in the way those cases require. Where, as here, an individual has not voluntarily conveyed information to a third party, her

expectation of privacy in that information is not defeated under the third-party doctrine. *See, e.g.*, *Third Circuit Opinion*, 620 F.3d at 317-18; *Tracey*, 152 So. 3d at 522.

d. Discarding or Turning Off Cell Phones Is Not a Viable Alternative

Faced with the Court's concerns over the acquisition of historical CSLI generated by passive conduct, the government offered an alternative: people need not carry a cell phone in the first place or they may keep it turned off. Hr'g Tr. at 17:11-18:13. This cannot be right. Individuals cannot be compelled to choose between maintaining their Fourth Amendment right to privacy in their location and using a device that has become so integral to functioning in today's society that the U.S. Supreme Court once quipped "the proverbial visitor from Mars might conclude [it was] an important feature of human anatomy." *Riley*, 134 S. Ct. at 2484.

For many, cell phones are not a luxury good; they are an essential part of living in modern society. As the U.S. Supreme Court stated in *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010), "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." As the U.S. Supreme Court explained in *Riley*, "it is the person who is not carrying a cell phone, with all that it contains, who is the exception." 134 S. Ct. at 2490. In fact, "more than 90% of American adults . . . own a cell phone," *id.*, and "there are now more cell phones than people in the United States," Shane Miller, *Drawing the Line: The Legality of Using Wiretaps to Investigate Insider Trading*, 13 U. Pitt. J. Tech. L. Pol'y 1, 2 (2013). Further, according to a poll cited in *Riley*, "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." *Riley*, 134 S. Ct. at 2490. Considering the ubiquity of cell phones, and the important role they play in today's world, it is untenable to force individuals to disconnect from society just so they can avoid having their movements subsequently tracked by the government.

Consequently, the Court agrees wholeheartedly with the Florida Supreme Court: "Requiring a cell phone user to turn off the cell phone just to assure privacy from governmental

intrusion that can reveal a detailed and intimate picture of the user's life places an unreasonable burden on the user to forego [sic] necessary use of his cell phone, a device now considered essential by much of the populace." *Tracey*, 152 So. 3d at 523; *see also In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011) ("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."); Patrick E. Corbett, *The Fourth Amendment and Cell Site Location Information: What Should We Do While We Wait for the Supremes?*, 8 Fed. Cts. L. Rev. 215, 226-27 (2015) (questioning whether requiring users to switch their cell phones off to avoid being tracked is a "viable option" given "the desire (and often need) to stay connected and informed"). In this regard, the Court takes heed of Judge Robin S. Rosenbaum's concurrence in *Davis*: "In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling." 785 F.3d at 525 (Rosenbaum, J., concurring).

e. Conclusion

For these reasons, the Court concludes that the third-party doctrine established in *Miller* and *Smith* does not defeat cell phone users' reasonable expectation of privacy in the historical CSLI associated with their cell phones. The government therefore conducts a "search" within the meaning of the Fourth Amendment when it asks cellular service providers to release that information pursuant to 18 U.S.C. § 2703.

C. Exceptions to the Warrant Requirement

Where, as here, "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing," the Fourth Amendment "generally requires the obtaining of a judicial warrant." *Riley*, 134 S. Ct. at 2482 (internal quotation marks omitted). "In the absence of a

warrant," the U.S. Supreme Court has held, "a search is reasonable only if it falls within a specific exception to the warrant requirement." *Id.*; *see also Karo*, 468 U.S. at 717 ("Warrantless searches are presumptively unreasonable, though the Court has recognized a few limited exceptions to this general rule.").

The only exception to the warrant requirement advanced by the government here is consent. It is well established that the government need not obtain a warrant when it has the consent of the individual whose person or property is to be searched. *See Karo*, 468 U.S. at 717 (recognizing consent as one of the "limited exceptions" to the Fourth Amendment's warrant requirement). "Consent searches are part of the standard investigatory techniques of law enforcement agencies" and are "a constitutionally permissible and wholly legitimate aspect of effective police activity." *Fernandez v. California*, 134 S. Ct. 1126, 1132 (2014).

The question here, then, is whether cell phone users have consented to the government's acquisition of the historical CSLI associated with their cell phones. Undoubtedly, this question bears some relation to the issue of voluntariness discussed in Part III.B.2, *supra*. The Court's focus here, however, will be on the privacy policies issued by the cellular service providers of the target cell phones identified in the government's application: Verizon and AT&T. The mere existence of a privacy policy, the Court notes, does not dispose of the consent inquiry for Fourth Amendment purposes. In *City of Ontario v. Quon*, for example, the U.S. Supreme Court assumed that a police officer "had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City," even though the department "made it clear that pager messages were not considered private" and "[t]he City's Computer Policy stated that 'users should have no expectation of privacy or confidentiality when using' City computers," including pagers. 560 U.S. at 758, 760 (brackets omitted).

Of primary concern to the Court is the fact that subscribers of Verizon and AT&T cannot possibly have consented to the government's acquisition of CSLI generated by their cell phones but collected by an entirely different provider. There are at least two reasons why another

provider might have collected historical CSLI for a Verizon or AT&T subscriber that the government has targeted. First, a provider other than Verizon or AT&T might have collected CSLI generated by a target cell phone if a target user switched providers during the sixty-day period but kept the same phone number pursuant to local number portability. App. ¶ 2 n.2. Second, a provider other than Verizon or AT&T might have collected CSLI generated by one of the target cell phones if a target cell phone connected with the cell tower of that other provider over the course of the sixty-day period, an action known as roaming. Larsen Decl. ¶ 2c. As stated above, roaming occurs when there is a gap in the network of a cell phone's provider and, as a result, the cell phone connects to the cell tower of a different provider.

As to roaming, which neither the Fifth Circuit nor the Eleventh Circuit addressed, the record before this Court indicates that "Verizon does retain CSLI for phone numbers belonging to other providers when those phones connect to Verizon towers." Larsen Decl. ¶ 2c. The same is true for AT&T, which "can determine whether [a] number [that is not an AT&T number] roamed on its system or called one of its customers and, if so, it can provide details of that usage, including CSLI."[11] *Id.* ¶ 4d. A cell phone user, however, will rarely know when she is roaming onto another provider's network of cell towers, and she will almost certainly not know the name of the other provider on whose network she is roaming. Even though the Court assumes that cell phone users have read the privacy policies of their own cellular service providers, users almost certainly do not read the privacy policies of every provider on whose towers their cell phones might roam. It cannot be, therefore, that the privacy policy of a user's cellular service provider offers a basis for that user to consent to the government's acquisition of CSLI from a separate provider.

What is more, the government says that, based on the language of the application, it "need

[11] The record also shows that "Sprint and Verizon have a roaming contract" whereby "Verizon sends a report of all roaming activity to Sprint's billing department." Larsen Decl. ¶ 3c. Sprint then bills its subscriber for roaming charges, but the subscriber's "bill does not contain CSLI." *Id.*

not seek a new application" in order to obtain historical CSLI associated with a target cell phone from any of the dozens of other cellular service providers listed in the application. Schenk Decl. ¶ 1a. This is true whether the government's basis for requesting historical CSLI from a separate provider is local number portability or roaming. *See id.*; App. ¶ 2 & n.2. The government's application therefore authorizes the government to obtain CSLI from a plethora of other cellular service providers, such as Cellular One, Sprint, and T-Mobile, to whom the target cell phone users could not possibly have provided their consent.

In fact, when the Court requested that the government provide "the most recent privacy policies for each Telephone Service Provider listed in the government's application," ECF No. 24, the government's response illustrated the implausibility of user consent:

> If in its Order for Supplemental Filings, this Court is seeking the most recent privacy policies for each Telephone Service Provider listed in the government's application, rather than the privacy policies for each Telephone Service Provider for each of the Target Devices, *that request is nearly without bound*, essentially requiring the privacy policies for *every service provider in the country*. Therefore, if the Court, in fact, wants the privacy policies for any and all telephone service providers, the government requests additional time to comply with this request, *assuming compliance is possible*.

ECF No. 29 at 2 (emphases added). How is it, then, that a cell phone user has consented to government acquisition of CSLI when, to do so, she would have had to read the privacy policy of "every service provider in the country," a task the government itself admits might not even be "possible"?

As for the privacy policies submitted by the government, the Court finds that they are sufficiently vague as to the nature and scope of the CSLI sought that subscribers cannot be said to have consented to that information's release to the government. Verizon's policy is especially vague. Verizon tells its subscribers, "We collect information about your use of our products, services and sites. Information such as . . . wireless location . . . ." Verizon Policy. "We may," Verizon says, "disclose information that individually identifies our customers or identifies customer devices in certain circumstances, such as: to comply with valid legal process including

subpoenas, court orders or search warrant."[12] *Id.* Verizon's privacy policy says nothing about how or when CSLI is generated.[13] There is no mention, for instance, that every call made or received, every text sent or received, and every data connection will generate CSLI. Nor is there mention of how accurate the vaguely worded "wireless location" information might be. Additionally, far from giving its subscribers any understanding of the length of time for which their location information will be stored, Verizon's policy states only: "Personally identifiable and other sensitive records are retained only *as long as reasonably necessary* for business, accounting, tax or legal purposes." *Id.* (emphasis added). The record does not establish how long "as long as reasonably necessary" is. The Court cannot conclude that such a policy provides the basis for consent to the government's acquisition of sixty days' worth of historical CSLI.

AT&T's policy fares no better. AT&T informs its subscribers that it will collect their "location information," which includes "the whereabouts of your wireless device." AT&T Policy. "Location information," AT&T's policy continues, "is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies, including the satellites that comprise the Global Positioning System." *Id.* The AT&T policy tells subscribers that AT&T "automatically collect[s] information" when they "use our network," and that AT&T may provide this information to "government agencies" in order to "[c]omply with court orders." *Id.* The policy also contains information regarding the accuracy of the "wireless location information" that AT&T collects, explaining that AT&T "can locate your device based on the cell tower that's serving you" up to 1,000 meters in urban areas and 10,000 meters in rural areas. *Id.*

At no point, however, does AT&T's privacy policy give the cell phone user any indication

---

[12] The mere mention of "court orders" in a privacy policy cannot provide a basis for consent. As the Verizon policy makes clear, cell phone users at most can consent to "valid" court orders—i.e., those that are not constitutionally infirm.

[13] The Fifth Circuit's brief analysis of privacy policies was limited to instances where cell phone users are making phone calls. *See Fifth Circuit Opinion*, 724 F.3d at 613. As explained earlier, the factual record here also includes CSLI generated by continuously running apps and automatic pinging, as well as the receipt of text messages. Verizon's policy gives the user no indication that any of these passive activities will generate CSLI.

as to how long AT&T will keep records of a subscriber's CSLI. In AT&T's letter to Congress, AT&T disclosed that it will store such data for five years. *See* ACLU Br. at 2 n.5 (citing Letter from Timothy P. McKone, Executive Vice President, AT&T, to Rep. Edward J. Markey (Oct. 3, 2013)). Subscribers would not know that from the privacy policy. As the AT&T policy says nothing about how long a cell phone user's CSLI will be stored, the Court cannot conclude that such a policy provides the basis for consent to the government's acquisition of sixty days' worth of historical CSLI.

In addition, nowhere does the Verizon or AT&T privacy policy indicate the volume of location data that is likely to be collected and stored by the provider. There is no estimate, for example, of the number of location data points a typical user will generate over the course of an hour, day, week, month, or year. This omission is especially problematic considering that the sheer volume of CSLI generated by a user's cell phone can be staggering. *See* Wessler Decl. ¶¶ 8-10. In *Davis*, for instance, the government obtained the defendant's CSLI for a period of sixty-seven days. "During that time, Davis made or received 5,803 phone calls, so the prosecution had 11,606 data points about Mr. Davis's location." *Davis*, 785 F.3d at 533 (Martin, J., dissenting). "This averages around one location data point every *five and one half minutes* for those sixty-seven days, assuming Mr. Davis slept eight hours a night." *Id.* at 540.

In light of the foregoing, the Court cannot conclude that cell phone users generally—or in this instance—consent through the privacy policies of their cellular service providers to the government's warrantless acquisition of the historical CSLI associated with the users' cell phones. Because the government offers no other basis for its conduct to be excepted from the Fourth Amendment's warrant requirement, the Court holds that the government must, pursuant to Rule 41 of the Federal Rules of Criminal Procedure, secure a warrant supported by probable cause in order to obtain a cell phone user's historical CSLI.

This requirement does not impose an undue burden on the government. Indeed, the SCA expressly contemplates that the government may need to "obtain[] a warrant issued using the

procedures described in the Federal Rules of Criminal Procedure" in order to acquire "a record or other information pertaining to a subscriber to or customer of [a provider of electronic communication service]." 18 U.S.C. § 2703(c)(1)(A). Further, although requiring a warrant for historical CSLI will surely have an impact on law enforcement practices, this requirement "is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow weighed against the claims of police efficiency.'" *Riley*, 134 S. Ct. at 2493 (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971)). It may be true that court orders for historical CSLI have served as "an investigative tool" used to establish probable cause in the past, Gov't Reply at 11, but the government is "not free from the warrant requirement merely because it is investigating criminal activity," *Third Circuit Opinion*, 620 F.3d at 318. "Recent technological advances," moreover, "have . . . made the process of obtaining a warrant itself more efficient." *Riley*, 134 S. Ct. at 2493; *see also Missouri v. McNeely*, 133 S. Ct. 1552, 1573 (2013) (Roberts, C.J., concurring in part and dissenting in part) (explaining that in some jurisdictions "police officers can e-mail warrant requests to judges' iPads; judges have signed such warrants and e-mailed them back to officers in less than 15 minutes").

Finally, the Court does not hold that the government may *never* obtain historical CSLI without a warrant supported by probable cause. It may be that "other case-specific exceptions," such as exigent circumstances, would "still justify a warrantless search" for historical CSLI. *Riley*, 134 S. Ct. at 2494. It may also be that historical CSLI acquired without a warrant is admissible at trial under the exclusionary rule's good faith exception. In general, however, if the government wants to obtain historical CSLI associated with a particular cell phone, the Fourth Amendment requires that the government secure a warrant before doing so.

D. Remedy

Having found that the Fourth Amendment generally requires that the government obtain a warrant supported by probable cause before acquiring a cell phone user's historical CSLI from a cellular service provider, the Court must address whether such a conclusion renders any part of the

SCA unconstitutional. The Court holds that it does not.

The Court agrees with Judge Illston that "the SCA makes no mention of cell site data, but rather speaks in general terms of 'records concerning electronic communication.'" *Cooper*, 2015 WL 881578, at *8. As a matter of statutory construction, "where an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988).

As stated earlier, the SCA provides, in relevant part:

> c) Records concerning electronic communication service or remote computing service.—
>
> (1) 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 (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;
>
> (B) obtains *a court order* for such disclosure *under subsection (d)* of this section.

18 U.S.C. § 2703(c)(1)(A)-(B) (emphases added). Subsection (d), referred to in § 2703(c)(1)(B), provides further:

> (d) Requirements for court order.—
>
> A court order for disclosure under subsection (b) or (c) 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.* In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Id. § 2703(d) (emphasis added).

In short, the government has two basic options for obtaining "a record or other information pertaining to a subscriber to or customer of [a provider of electronic communication service]," such as historical CSLI. 18 U.S.C. § 2703(c)(1). Those options are: (1) a search warrant supported by probable cause, *id* § 2703(c)(1)(A); or (2) a court order under § 2703(d) based on specific and articulable facts showing that the information sought is relevant and material to an ongoing criminal investigation, *id.* § 2703(c)(1)(B). It is less than clear why Congress created two different paths. Perhaps, as Judge Lloyd suggests, Congress did so out of "recognition that some information should be accorded a higher level of protection from disclosure than other information." ECF No. 2 at 4. In any event, all the Court holds today is that when the government seeks to obtain historical CSLI from a cellular service provider, the Fourth Amendment requires that the government obtain a warrant. To do so, the government need only follow the procedures already outlined in § 2703(c)(1)(A).

The language of § 2703(d) is not to the contrary. Section 2703(d) provides that a "court order for disclosure under subsection (b) or (c) *may be issued* by any court that is a court of competent jurisdiction and *shall issue only if"* the specific and articulable facts standard is met. 18 U.S.C. § 2703(d) (emphases added). If, as the government contends, the language of § 2703(d) *requires* a magistrate judge to issue a court order so long as the government has met the specific and articulable facts standard, a standard lower than probable cause, then § 2703(d) of the SCA would be unconstitutional as applied to historical CSLI. *See* Gov't Reply at 12.

This Court, however, finds that the Third Circuit's interpretation of § 2703(d) is an acceptable construction of the provision such that it need not be invalidated. *See Third Circuit Opinion*, 620 F.3d at 315-17. The Third Circuit held that § 2703(d) provides magistrate judges with discretion to require a warrant on a showing of probable cause because that provision begins with the permissive language "may be issued" and uses the phrase "only if," rather than simply "if." *Id.* at 315. The Third Circuit found that if issuing an order under § 2703(d) were not discretionary, "the word 'only' would be superfluous." *Id.* This is so, the Third Circuit reasoned,

because "the phrase 'only if' describe[s] a necessary condition, not a sufficient condition" for obtaining a § 2703(d) order. *Id.* at 316 (internal quotation marks omitted). The Third Circuit explained:

> Adopting the example of the baseball playoffs and World Series, we noted that while a team may win the World Series *only if* it makes the playoffs[,] a team's meeting the necessary condition of making the playoffs does not guarantee that the team will win the World Series. In contrast, winning the division is a sufficient condition for making the playoffs because a team that wins the division is ensured a spot in the playoffs and thus a team makes the playoffs *if* it wins its division.

Id. (citations, alterations, and internal quotation marks omitted).

Because a showing of specific and articulable facts is a necessary, rather than a sufficient, condition for obtaining a § 2703(d) order, magistrate judges have discretion to require a higher threshold where the Constitution so requires. *See Third Circuit Opinion*, 620 F.3d at 315 (agreeing that "the requirements of § 2703(d) merely provide a floor—the minimum showing required of the Government to obtain the information—and that magistrate judges do have discretion to require warrants"). The lesser showing of specific and articulable facts may well be sufficient to obtain stored electronic information under § 2703(d) that, unlike historical CSLI, does not raise constitutional privacy concerns. Here, however, where the information sought is historical CSLI, a warrant supported by probable cause is required, and the government is not foreclosed from proceeding under § 2703(d) so long as the probable cause standard is met. To avoid unnecessary confusion, though, the government should request historical CSLI under § 2703(c)(1)(A), which expressly mentions "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure."

IV. CONCLUSION

For the foregoing reasons, the Court hereby AFFIRMS Judge Lloyd's denial of the government's application for historical CSLI.

IT IS SO ORDERED.

Dated: July 29, 2015

LUCY H. KOH
United States District Judge