No. 15-146

IN THE

Supreme Court of the United States

QUARTAVIOUS DAVIS,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

SUPPLEMENTAL BRIEF FOR PETITIONER

Steven R. Shapiro
Nathan Freed Wessler
Jameel Jaffer
Ben Wizner
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

Nancy Abudu
ACLU FOUNDATION OF FLORIDA, INC.
4500 Biscayne Boulevard, Suite 340
Miami, FL 33137

Benjamin James Stevenson
ACLU FOUNDATION OF FLORIDA, INC.
P.O. Box 12723
Pensacola, FL 32591-2723

David Oscar Markus
Counsel of Record
MARKUS/MOSS PLLC
40 N.W. 3rd Street, Penthouse One
Miami, FL 33128
(305) 379-6667
dmarkus@markuslaw.com

Jacqueline E. Shapiro
40 N.W. 3rd Street, Penthouse One
Miami, FL 33128

Attorneys for Petitioner

TABLE OF CONTENTS

SUPPLEMENTAL BRIEF FOR PETITIONER

Pursuant to Rule 15.8, Petitioner Quartavius Davis respectfully submits this supplemental brief to call the Court's attention to a recent decision by the Fourth Circuit, issued after the filing of the Petition in this case, that squarely conflicts with the Eleventh Circuit's decision below, thus widening the circuit split and providing a further compelling reason for this Court to grant certiorari. A copy of the Fourth Circuit's decision in *United States v. Graham*, No. 12-4825, __ F.3d __, 2015 WL 4637931 (4th Cir. Aug. 5, 2015), is set out in the attached Supplemental Appendix 1a–117a.

In *Graham*, as here, law enforcement officials engaged in a criminal investigation obtained historical cell site location information ("CSLI") from cellular service providers pursuant to an order under the Stored Communications Act, 18 U.S.C. § 2703(d), rather than a probable cause warrant. *Id.* at 15a–16a. The government in *Graham* obtained two sets of CSLI pursuant to successive 2703(d) orders, one covering 14 days and the other 221 days (approximately seven months). *Id.* at 16a. In this case, the government obtained 67 days of Petitioner's CSLI. Pet. App 7a–8a.

Presented with the same legal question, the Fourth Circuit's decision in *Graham* conflicts with the Eleventh Circuit's holding in this case on two critical issues: first, whether law enforcement's acquisition of a person's historical CSLI from his or her cellular service provider is a Fourth Amendment search, and second, if it is a search, whether that search requires a warrant.

1. By holding that "the government engages in a Fourth Amendment search when it seeks to examine historical CSLI pertaining to an extended time period like 14 or 221 days," Supp. App. 29a, the Fourth Circuit's ruling in *Graham* conflicts with the holdings of the Eleventh Circuit in this case and the Fifth Circuit in *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013), and *United States v. Guerrero*, 768 F.3d 351 (5th Cir. 2014).

In reaching its conclusion, the Fourth Circuit first explained that government acquisition of historical CSLI impinges on expectations of privacy because, "[m]uch like long-term GPS monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life." Supp. App. 25a; *see also id.* at 26a ("[E]xamination of historical CSLI can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home."). The Eleventh Circuit reached a different conclusion, opining both that "[h]istorical cell site location data does not paint [an] 'intimate portrait of personal, social, religious, medical, and other activities and interactions,'" and that the expectation of privacy in CSLI "do[es] not turn on the quantity" or duration of records collected. Pet. App. 36a.

The Fourth Circuit went on to hold that this expectation of privacy is not vitiated merely because the CSLI records are held in trust by a service provider: "We decline to apply the third-party doctrine in the present case because a cell phone user

does not 'convey' CSLI to her service provider at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement." Supp. App. 38a. "We conclude, in agreement with the analysis of the Third Circuit in In re Application (Third Circuit) and that of several state supreme courts, that the third-party doctrine of Smith and Miller does not apply to CSLI generated by cell phone service providers." *Id.* at 40a (citing *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 317 (3d Cir. 2010); *Commonwealth v. Augustine*, 4 N.E.3d 846, 862–63 (Mass. 2014); *Tracey v. State*, 152 So. 3d 504, 525 (Fla. 2014); *State v. Earls*, 70 A.3d 630, 641–42 (N.J. 2013)). The Fourth Circuit explicitly detailed its disagreement with the Fifth and Eleventh Circuits on this point, explaining that "[p]eople cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones." *Id.* at 42a. The Fourth Circuit's opinion in *Graham* thus sharpens the circuit splits previously identified by Petitioner. *See* Pet. 22–28.

2. The Fourth Circuit also split with the Eleventh Circuit's novel conclusion that even if "government acquisition of CSLI through use of a 2703(d) order is a Fourth Amendment search, such a search would be reasonable under the Fourth Amendment and not require a warrant." Supp. App. 18a n.2 (citing *United States v. Davis*, 785 F. 3d 498, 516–18 (11th Cir. 2015) (en banc)). As the Fourth Circuit held,

> Section 2703(d) orders, as previously noted, do not require a showing of probable cause and do not fit within any of the "well delineated exceptions" to the general rule that a search requires a warrant based on probable cause. [*City of Ontario, Cal. v.*] *Quon*, 560 U.S. [746,] 760 [(2010)]. We decline here to create a new exception to a rule so well established in the context of criminal investigations.

Id. As explained in the petition, the Eleventh Circuit's holding on this point is at odds with the precedents of numerous courts, including this one. *See* Pet. 28, 34–35.

3. The Fourth Circuit is not the only federal court to have held since filing of the petition in this case that a warrant is required for law enforcement access to historical CSLI. On July 29, 2015, Judge Lucy H. Koh of the U.S. District Court for the Northern District of California decided *In re Application for Telephone Information Needed for a Criminal Investigation*, No. 15-XR-90304, 2015 WL 4594558 (N.D. Cal. July 29, 2015) (public redacted version). Supp. App. 118a–182a. Like the Fourth Circuit, that court held that historical CSLI receives the full protection of the Fourth Amendment, and disagreed with the Eleventh Circuit's reasoning in *Davis*.

4. The issues in this case have been fully aired by lower courts, and are ripe for this Court's decision. Indeed, as both the majority and dissenting opinions in *Graham* recognize, the questions presented require resolution by this Court. Writing for the

Fourth Circuit majority, Judge Davis noted that "[i]f the Twenty–First Century Fourth Amendment is to be a shrunken one, as the dissent proposes, we should leave that solemn task to our superiors in the majestic building on First Street and not presume to complete the task ourselves." Supp. App. 53a. In dissent, Judge Motz suggested that, though she felt bound by her interpretation of this Court's third-party records cases, it may be time for this Court to revisit those opinions and clarify the state of the law. *Id.* 117a. Because the issues in this case are of national importance, and because the circuits are split, this Court should accept the case for review.

CONCLUSION

For the foregoing reasons, and for the reasons stated in the petition for a writ of certiorari, the petition should be granted.

Respectfully Submitted,

David Oscar Markus
Counsel of Record
MARKUS/MOSS PLLC
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128
(305) 379-6667
dmarkus@markuslaw.com

Jacqueline E. Shapiro
40 N.W. 3rd Street,
Penthouse One
Miami, FL 33128

Steven R. Shapiro
Nathan Freed Wessler
Jameel Jaffer
Ben Wizner
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004

Nancy Abudu
ACLU FOUNDATION OF
FLORIDA, INC.
4500 Biscayne Blvd.,
Ste. 340
Miami, FL 33137

Benjamin James Stevenson
ACLU FOUNDATION OF
FLORIDA, INC.
P.O. Box 12723
Pensacola, FL 32591-2723

Dated: August 19, 2015

APPENDIX

UNITED STATES COURT OF APPEALS
FOR THE FOURT CIRCUIT

No. 12-4659

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

AARON GRAHAM,
Defendant-Appellant.

ELECTRONIC FRONTIER FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS; AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND; CENTER FOR DEMOCRACY & TECHNOLOGY; AMERICAN CIVIL LIBERTIES UNION FOUNDATION,

Amici Supporting Appellant.

No. 12-4825

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

ERIC JORDAN,
Defendant-Appellant.

ELECTRONIC FRONTIER FOUNDATION; NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS; AMERICAN CIVIL

LIBERTIES UNION FOUNDATION OF MARYLAND; CENTER FOR DEMOCRACY & TECHNOLOGY; AMERICAN CIVIL LIBERTIES UNION FOUNDATION,

Amici Supporting Appellant.

Appeals from the United States District Court for the District of Maryland, at Baltimore. Richard D. Bennett, District Judge. (1:11-cr-00094-RDB-1; 1:11-cr-00094-RDB-2)

Argued: December 11, 2014 Decided: August 5, 2015

Before MOTZ and THACKER, Circuit Judges, and DAVIS, Senior Circuit Judge.

Affirmed by published opinion. Senior Judge Davis wrote the majority opinion, in which Judge Thacker joined. Judge Thacker wrote a separate concurring opinion. Judge Motz wrote an opinion dissenting in part and concurring in the judgment.

ARGUED: Meghan Suzanne Skelton, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Greenbelt, Maryland; Ruth J. Vernet, RUTH J VERNET, ESQ., LLC, Rockville, Maryland, for Appellants. Rod J. Rosenstein, OFFICE OF THE UNITED STATES ATTORNEY, Baltimore, Maryland, for Appellee. **ON BRIEF**: James Wyda, Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Baltimore, Maryland, for Appellant Aaron Graham. Nathan Judish, Computer Crime & Intellectual

Property Section, UNITED STATES DEPARTMENT OF JUSTICE, Washington, D.C.; Benjamin M. Block, Assistant United States Attorney, Baltimore, Maryland, Sujit Raman, Chief of Appeals, OFFICE OF THE UNITED STATES ATTORNEY, Greenbelt, Maryland, for Appellee. Nathan Freed Wessler, Catherine Crump, Ben Wizner, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, New York, New York; David R. Rocah, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF MARYLAND, Baltimore, Maryland; Kevin S. Bankston, Gregory T. Nojeim, CENTER FOR DEMOCRACY & TECHNOLOGY, Washington, D.C.; Thomas K. Maher, Vice-Chair, 4th Circuit Amicus Committee, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, Durham, North Carolina; Hanni Fakhoury, ELECTRONIC FRONTIER FOUNDATION, San Francisco, California, for Amici Curiae.

DAVIS, Senior Circuit Judge:

Appellants Aaron Graham and Eric Jordan appeal their convictions for several offenses arising from a series of armed robberies. Specifically, Appellants challenge the district court's admission of testimonial and documentary evidence relating to cell site location information ("CSLI") recorded by their cell phone service provider. We conclude that the government's warrantless procurement of the CSLI was an unreasonable search in violation of Appellants' Fourth Amendment rights. Nevertheless, because the government relied in good faith on court orders issued in accordance with Title II of the Electronic Communications Privacy Act, or the Stored Communications Act ("SCA"), we hold the

court's admission of the challenged evidence must be sustained.

Jordan separately challenges restrictions on his own testimony imposed by the district court, the court's denial of his motion for severance, the exclusion of certain out-of-court statements attributed to Graham, the admission of evidence seized during a search of his residence, and the sufficiency of the evidence supporting several of his convictions. Finding no reversible error in these respects, we affirm the judgment of the district court.

I.

This prosecution arose from a series of six armed robberies of several business establishments located in Baltimore City and Baltimore County, Maryland. After a nine-day joint trial in the U.S. District Court for the District of Maryland, a jury found Appellants guilty on all counts submitted to it. Aaron Graham was convicted of being a felon in possession of a firearm, Hobbs Act robbery, conspiracy to commit Hobbs Act robbery, and brandishing a firearm in connection with all six robberies. Eric Jordan was convicted of conspiracy, Hobbs Act robbery, and brandishing a firearm in connection with three of the robberies.

A.

The evidence adduced at trial permitted the jury to find the following facts.

The first robbery occurred the evening of January 17, 2011, at a Dollar Tree store in Baltimore County. Graham entered the store, brandished a small black gun, and directed a cashier to open a

cash register. The cashier removed cash from the register and gave it to Graham. Graham reached over the counter to grab additional cash before fleeing the store.

The second and third robberies occurred five days later. On the evening of January 22, 2011, five individuals, including Graham, arrived at Mondawmin Mall in Baltimore in a dark colored Ford F-150 pickup truck, exited the vehicle, and entered the shopping mall before the truck pulled away. Graham, seen on video surveillance wearing the same clothing worn during the Dollar Tree robbery five days earlier, entered the Milan Gold & Diamonds jewelry store ("Milan Gold") inside the mall with a second individual. After two other individuals entered the store, leaving a fifth standing outside the door, Graham pointed a gun at a clerk and demanded, "Don't be smart with me. Just give me everything." J.A. 1522. The three persons with Graham picked up the jewelry as the clerk removed it from a display case. Graham demanded a specific watch from a separate display case and, after the clerk gave it to him, he and the others left the mall.

Later that evening, Graham, again wearing the same clothes, entered a 7-Eleven store in Baltimore, walked behind the counter, grabbed the clerk, and demanded that he open the cash register. The clerk did not see a gun but saw Graham's hand inside his jacket and later testified that "it felt like there was some kind of weapon, some kind of material in there . . . ." J.A. 1600. Graham emptied two cash registers and then ordered the clerk to go into a back room inside the store. After Graham left, the clerk observed Graham enter the driver's side of

an F-150 truck and depart. The clerk recorded video of the truck pulling away and its appearance matched that of the truck used at Mondawmin Mall earlier that evening.

The fourth robbery occurred on February 1, 2011, at a Shell gas station in Baltimore County. Graham and a masked individual entered the cashier's booth, where Graham pushed the clerk to the floor, began punching and kicking him, and then brandished a small gun, placing it near the clerk's ear. Meanwhile, a third individual stood near the door to the store with a sawed-off shotgun. When a customer attempted to leave, the third robber blocked the exit, forced the customer to the ground, and beat him in the head with the shotgun. After Graham and the second robber removed cash from the booth, the three robbers departed.

The fifth and sixth robberies occurred four days later. On February 5, 2011, at approximately 3:29 p.m., Graham entered a Burger King restaurant in Baltimore wearing the same jacket worn during the Dollar Tree, Milan Gold, and 7-Eleven robberies, and carrying a small black gun with a white handle. Graham brandished the weapon and demanded money. The restaurant manager opened several cash registers, which Graham emptied before departing. Graham was seen entering a dark colored F-150 truck on the passenger side before the truck pulled away.

About forty five minutes later, Graham entered a McDonald's restaurant approximately two miles from the Burger King, went behind the counter, and demanded money, brandishing a small black gun with a white handle. After the restaurant

manager opened three cash registers, Graham removed cash and stuffed it into his jacket before departing. The manager saw Graham enter the passenger side of a dark pickup truck, which pulled away rapidly.

While investigating the Burger King robbery, Officer Joshua Corcoran of the Baltimore Police Department received reports describing the robber, his clothing, and the pickup truck. Shortly thereafter, he heard a radio call regarding the McDonald's robbery and indicating that the pickup truck was possibly headed toward his location.

After leaving the Burger King, Corcoran spotted a pickup truck matching the descriptions he received and observed that a passenger inside the vehicle wore a jacket matching the description of that reportedly worn by the Burger King robber. During Corcoran's pursuit of the truck, the driver drove it up onto a sidewalk and accelerated. Corcoran continued pursuit just before the truck became trapped between heavy traffic, a construction barrier, and a moving train in front of it, and was forced to stop.

Corcoran and another officer conducted a felony car stop, directing orders to Graham and the driver, Jordan. Graham and Jordan were non-compliant with some of the officers' instructions but were eventually secured and arrested. At the scene, employees of Burger King and McDonald's identified Graham as the robber. A black .25 caliber Taurus pistol with a pearl handle was recovered from under the passenger seat. Nearly $1,100 in cash bundles were recovered from the person of Graham and Jordan, and from an open console inside the truck.

B.

During the ensuing, post-arrest investigation, Detective Chris Woerner recognized similarities between the restaurant robberies and the Milan Gold and 7-Eleven robberies. Woerner prepared search warrants for Graham's and Jordan's residences and the pickup truck. The probable cause portion of each of the warrant affidavits described what was known at the time about the Milan Gold, 7-Eleven, Burger King, and McDonald's robberies. The search warrants were issued by a judge of the Circuit Court of Maryland for Baltimore City.

While Woerner was seeking the warrant for Graham's residence, other officers conducted a search of Jordan's apartment, recovering a sawed-off shotgun, a matching shotgun shell, a .357 caliber Rossi revolver, .357 caliber cartridges, and other items. Woerner executed searches of Graham's residence and the pickup truck, recovering a gun holster and several rings and watches from the residence, and two cell phones from the truck. After Woerner obtained warrants for the phones, the phone numbers associated with each phone was determined and matched the respective numbers disclosed by Graham and Jordan after their arrest.

Woerner contacted the Baltimore County Police Department to determine whether they were investigating any potentially related robberies, sending photos of Graham and Jordan and photos from the searches. Detective Kelly Marstellar recognized similarities to the Dollar Tree and Shell station robberies, including the similarity between the jacket worn by Jordan at the time of his arrest and that worn by the masked robber of the Shell

station, who had entered the cashier booth. The Baltimore County Police Department prepared and executed a second round of search warrants at Graham's and Jordan's residences on February 23, 2011. During the second search of Jordan's apartment, officers recovered clothing that matched that worn by Graham during the Shell station robbery.

The government sought cell phone information from Sprint/Nextel, the service provider for the two phones recovered from the truck. Sprint/Nextel identified Graham's phone as subscribed to Graham's wife at their shared Baltimore County address and Jordan's phone as subscribed to an alias or proxy. The government then sought and obtained two court orders for disclosure of CSLI for calls and text messages transmitted to and from both phones. The government's initial application for a court order sought CSLI for four time periods: August 10-15, 2010; September 18-20, 2010; January 21-23, 2011; and February 4-5, 2011. A second application followed, seeking information for a much broader timeframe: July 1, 2010 through February 6, 2011. The government used the court order to obtain from Sprint/Nextel records listing CSLI for this 221-day time period.

C.

The government charged Graham and Jordan with multiple counts of being felons in possession of a firearm, see 18 U.S.C. § 922(g)(1) (2011); robbery affecting commerce, see 18 U.S.C. § 1951(a) (Hobbs Act); conspiracy to commit Hobbs Act robbery, see id.; brandishing a firearm during a crime of violence, see 18 U.S.C. § 924(c); and conspiracy to brandish a

firearm during a crime of violence, see 18 U.S.C. § 924(o). Jordan was also charged with possession of an unregistered sawed-off shotgun. See 18 U.S.C. § 5861(d). The indictment also charged aiding and abetting the felon-in-possession, Hobbs Act robbery, conspiracy, and brandishing-a-firearm offenses. See 18 U.S.C. § 2. Graham was charged in connection with all six robberies, and Jordan was charged in connection with the Shell, Burger King, and McDonald's robberies.

Appellants filed a number of pre-trial motions, including motions for severance under Rule 14 of the Federal Rules of Criminal Procedure and a motion to suppress the CSLI obtained from Sprint/Nextel on Fourth Amendment grounds. Jordan separately filed a motion to suppress evidence seized during the search of his apartment, arguing that the first search warrant was defective. The district court denied all of Appellants' motions, and the case proceeded to trial.

During trial, Appellants objected to proposed testimony regarding CSLI from a Sprint/Nextel records custodian and from an FBI agent who investigated the case, arguing that the proposed testimony was impermissible expert opinion. The district court disagreed and admitted the proposed testimony. Jordan also filed a motion in limine seeking to admit a handwritten statement purportedly written by Graham and a recorded telephone call in which Graham participated. The court denied the motion, excluded the handwritten statement as hearsay and unauthenticated, and excluded the phone call as irrelevant. The court also ordered that the scope of Jordan's testimony be

limited to exclude certain irrelevant topics that were potentially prejudicial to Graham.

At the close of the government's case, the government moved to dismiss the count of conspiracy to possess a firearm during a crime of violence. Graham and Jordan moved for judgment of acquittal as to all remaining counts for insufficiency of evidence under Rule 29(a) of the Federal Rules of Criminal Procedure. The court denied the defendants' Rule 29(a) motions, except with respect to the felon-in-possession count, which the court granted as to Jordan.

Jordan's defense case consisted of his own testimony as well as that of four character witnesses and a private investigator. Graham declined to testify and offered no evidence.

The parties rested on April 26, 2012, and delivered closing arguments the following day. On April 30, 2012, the jury returned guilty verdicts on all remaining counts. Graham and Jordan submitted motions for new trials, which the district court denied. This appeal followed.

D.

During the pendency of this appeal, prior to oral argument, this Court directed each party to file a supplemental brief addressing the U.S. Supreme Court's recent decision in Riley v. California, 134 S. Ct. 2473 (2014), and permitted Appellants to file a supplemental reply brief. Dkt. No. 135. Appellants filed their supplemental brief on July 18, 2014, Dkt. No. 138; the government filed its supplemental response brief on August 4, 2014, Dkt. No. 142; and

Appellants filed a supplemental reply brief on August 8, 2014, Dkt. No. 144.

On August 21, 2014, the government filed a letter with the Court requesting permission to identify what it called "erroneous factual assertions" in Appellants' supplemental reply and seeking to rebut several assertions made in that brief. Dkt. No. 145. The next day, Appellants filed a motion to strike the government's letter as a sur-reply, Dkt. No. 146, to which the government did not respond.

The government's submission is, in effect, a sur-reply brief in the form of a letter. This Court does not generally permit the filing of sur-reply briefs without first granting leave for such a filing. Moreover, the government's letter fails to make an adequate demonstration of the need for a sur-reply. Accordingly, we grant the motion to strike, deny the government's request, and do not consider the content of the government's letter in disposition of this appeal.

E.

Graham and Jordan present several issues on appeal, arguing that the district court erred in admitting the government's CSLI evidence and certain testimony of the case agent and the Sprint/Nextel records custodian regarding the CSLI. Jordan argues separately that the district court also committed constitutional error in restricting his testimony and erred in denying his severance motion, excluding the out-of-court statements attributed to Graham, and admitting evidence seized from his apartment. Jordan argues further that the evidence presented at trial was insufficient to support

convictions for conspiracy, Hobbs Act robbery, or brandishing a firearm during a crime of violence. We consider these issues in turn.

II.

During the investigation of the robberies charged in this case, the government secured court orders under the SCA for 221 days' worth of historical CSLI from Sprint/Nextel. Appellants filed a motion to suppress use of the CSLI at trial, arguing that the government's acquisition of the records without a warrant based on probable cause was an unreasonable search in violation of the Fourth Amendment. The district court denied the motion, holding that the government's conduct was not an unreasonable search and, even if it was, the good-faith exception to the exclusionary rule justified admission of the CSLI. See generally United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012). The government ultimately used the CSLI at trial to establish Appellants' locations at various times before and after most of the charged robberies.

Appellants now appeal the denial of their motion to suppress. We review a district court's evidentiary rulings for abuse of discretion, United States v. Rivera, 412 F.3d 562, 566 (4th Cir. 2005), but we review de novo any legal conclusions as to whether certain law enforcement conduct infringes Fourth Amendment rights, United States v. Breza, 308 F.3d 430, 433 (4th Cir. 2002).

For the reasons explained below, we hold that the government's procurement of the historical CSLI at issue in this case was an unreasonable search. Notwithstanding that conclusion, we affirm the

district court's denial of the suppression motion because, in obtaining the records, the government acted in good-faith reliance on the SCA and the court orders issued under that statute.

A.

Historical CSLI identifies cell sites, or "base stations," to and from which a cell phone has sent or received radio signals, and the particular points in time at which these transmissions occurred, over a given timeframe. Cell sites are placed at various locations throughout a service provider's coverage area and are often placed on towers with antennae arranged in sectors facing multiple directions to better facilitate radio transmissions. A cell phone connects to a service provider's cellular network through communications with cell sites, occurring whenever a call or text message is sent or received by the phone.[1] The phone will connect to the cell site with which it shares the strongest signal, which is typically the nearest cell site. The connecting cell site can change over the course of a single call as the phone travels through the coverage area. When the phone connects to the network, the service provider automatically captures and retains certain information about the communication, including identification of the specific cell site and sector through which the connection is made.

[1] A "smartphone," a type of cell phone with a computer operating system, may communicate more frequently with the network than other types of cell phones through, for example, automatic updates to email inboxes and other operations of software applications installed on the phone.

By identifying the nearest cell tower and sector, CSLI can be used to approximate the whereabouts of the cell phone at the particular points in time in which transmissions are made. The cell sites listed can be used to interpolate the path the cell phone, and the person carrying the phone, travelled during a given time period. The precision of this location data depends on the size of the identified cell sites' geographical coverage ranges. Cell sites in urban areas, which have the greatest density of cell sites, tend to have smaller radii of operability than those in rural areas. The cell sites identified in the CSLI at issue in this case covered areas with a maximum radius of two miles, each divided into three 120-degree sectors.

B.

The government obtained Appellants' CSLI through use of court orders issued under the SCA directing Sprint/Nextel to disclose the information. The SCA "provid[es] an avenue for law enforcement entities to compel a provider of electronic communication services to disclose the contents and records of electronic communications." In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d) (In re Application (Fourth Circuit)), 707 F.3d 283, 287 (4th Cir. 2013); see also 18 U.S.C. §§ 2701–2711 (2010). The statute outlines procedures a governmental entity must follow to procure information from a service provider, treating subscriber account records differently than the content of electronic communications. United States v. Clenney, 631 F.3d 658, 666 (4th Cir. 2011) (citing 18 U.S.C. § 2703).

Absent subscriber notice and consent, the government must secure a warrant or a court order for subscription account records. 18 U.S.C. § 2703(c)(1). A warrant from a federal district court for the disclosure of subscriber records must be issued pursuant to the Federal Rules of Criminal Procedure, id. § 2703(c)(1)(A), which, in accordance with the Fourth Amendment, require a finding of probable cause by an impartial magistrate, Fed. R. Crim. P. 41(d); see also Payton v. New York, 445 U.S. 573, 588 n.26 (1980).

Section 2703(d) sets out the requirements for a court order for a service provider to disclose subscriber account records. The government must "offer[] specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). "This is essentially a reasonable suspicion standard[,]" In re Application (Fourth Circuit), 707 F.3d at 287, in contrast to the substantially higher probable cause standard for securing a warrant. The statute offers no express direction as to when the government should seek a warrant versus a § 2703(d) order.

The government obtained two § 2703(d) court orders for the CSLI at issue in this appeal. The first order directed Sprint/Nextel to disclose CSLI records for four time periods amounting to 14 days, and the second order directed disclosure of records for a much broader 221-day time period that included the previously ordered 14 days. Sprint/Nextel disclosed to the government the total 221 days' worth of CSLI for each Appellant's phone.

C.

Appellants argue that the government violated the Fourth Amendment in seeking and inspecting the CSLI at issue here without a warrant based on probable cause. We agree.

The Fourth Amendment protects individuals against unreasonable searches and seizures. Katz v. United States, 389 U.S. 347, 353 (1967). A "search" within the meaning of the Fourth Amendment occurs where the government invades a matter in which a person has an expectation of privacy that society is willing to recognize as reasonable. Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing Katz, 389 U.S. at 361 (Harlan, J., concurring)). A person's expectation of privacy is considered reasonable by societal standards when derived from "'concepts of real or personal property law or . . . understandings that are recognized and permitted by society.'" Minnesota v. Carter, 525 U.S. 83, 88 (1998) (quoting Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978)). Warrantless searches are, "as a general matter, . . . per se unreasonable under the Fourth Amendment," although "there are a few specifically established and well-delineated exceptions to that general rule." United States v. (Earl Whittley) Davis, 690 F.3d 226, 241-42 (4th Cir. 2012) (quoting City of Ontario, Cal. v. Quon, 560 U.S. 746, 760 (2010)) (internal quotation marks omitted).

We hold that the government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time. Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user

across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information. Its inspection by the government, therefore, requires a warrant, unless an established exception to the warrant requirement applies.[2]

1.

As an initial matter, we are not persuaded that, as the district court stated, Sprint/Nextel's privacy policy disproves Appellants' claim that they had an actual expectation in the privacy of their location and movements. The privacy policy in effect at the time Sprint/Nextel disclosed CSLI to the government stated as follows:

> Information we collect when we provide you with Services includes when your wireless device is turned on, how your device is functioning, device signal strength, where it is located, what device you are using, what you have

[2] The en banc Eleventh Circuit recently held that, assuming government acquisition of CSLI through use of a § 2703(d) order is a Fourth Amendment search, such a search would be reasonable under the Fourth Amendment and not require a warrant. United States v. (Quartavious) Davis, 785 F.3d 498, 516-18 (11th Cir. 2015) (en banc). Section 2703(d) orders, as previously noted, do not require a showing of probable cause and do not fit within any of the "well delineated exceptions" to the general rule that a search requires a warrant based on probable cause. Quon, 560 U.S. at 760. We decline here to create a new exception to a rule so well established in the context of criminal investigations.

> purchased with your device, how you are using it, and what sites you visit.

J.A. 957. First, the policy only states that Sprint/Nextel collects information about the phone's location – not that it discloses this information to the government or anyone else.

Second, studies have shown that users of electronic communications services often do not read or understand their providers' privacy policies.[3] There is no evidence that Appellants here read or understood the Sprint/Nextel policy.

2.

The Supreme Court has recognized an individual's privacy interests in comprehensive accounts of her movements, in her location, and in the location of her personal property in private spaces, particularly when such information is available only through technological means not in use by the general public.

a.

In United States v. Knotts, 460 U.S. 276 (1983), law enforcement officers used a combination of visual surveillance and monitoring of a radio transmitter installed in a container of chloroform to track the container's movements by automobile to

---

[3] See, e.g., Federal Trade Commission, Mobile Privacy Disclosures: Building Trust Through Transparency 10 (Feb. 2013), http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf (saved as ECF opinion attachment); Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J. L. & Pol'y Info. Soc'y 543, 544 (2008).

the defendants' homes. 460 U.S. at 278-79. In holding that this practice did not infringe upon a reasonable expectation of privacy, the Court emphasized the "limited" nature of the government's electronic surveillance effort, which was confined to tracking the container's movement on public roads from its place of purchase to its ultimate destination. Id. at 284. Although the government tracked the container to a defendant's private home, there was no indication that the officers continued to monitor the container inside the private space after its public journey had ended. Id. at 285; see also California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.").

Knotts left unanswered two questions critical to assessing the constitutionality of the government's conduct in the present case: (1) whether tracking the location of an individual and her property inside a private space constitutes a Fourth Amendment search; and (2) whether locational tracking of an individual and her property continuously over an extended period of time constitutes a search. Courts have answered each of these questions in the affirmative.

b.

United States v. Karo, 468 U.S. 705 (1984), addressed the first question. As in Knotts, government agents surreptitiously used a radio transmitter to track the movements of a chemical container to a private residence, but here the agents continued to monitor the container while it was

inside the residence. Karo, 468 U.S. at 709-10. The Court held that this practice "violate[d] the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." Id. at 714. The government's monitoring of the beeper "reveal[ed] a critical fact about the interior of the premises . . . that [the government] could not have otherwise obtained without a warrant": "that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched." Id. at 715. "Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight." Id. at 716 (footnote omitted).

In Kyllo v. United States, 533 U.S. 27 (2001), the Court again considered whether the use of technology to discover information hidden in a private home constituted a Fourth Amendment search. The government aimed a thermal imaging device at the petitioner's home from a public street to detect infrared radiation inside the home, which would allow it to identify the locations and movements of persons and certain objects inside. Id. at 29-30. The Court held that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." Id. at 40.

Like the searches challenged in Karo and Kyllo, examination of historical CSLI can allow the government to place an individual and her personal property – specifically, her cell phone – at the person's home and other private locations at specific points in time. "In the home, . . . all details are intimate details, because the entire area is held safe from prying government eyes." Id. at 37; see also Karo, 468 U.S. at 714 ("[P]rivate 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."). The Karo and Kyllo Courts recognized the location of a person and her property within a home at a particular time as a "critical" private detail protected from the government's intrusive use of technology. See Kyllo, 533 U.S. at 37; Karo, 468 U.S. at 715.

Inspection of long-term CSLI invades an even greater privacy interest than the search challenged in Karo because, unlike a cell phone, the tracking device in Karo was not carried on anyone's person and therefore was not capable of tracking the location of any individual. Additionally, the private location information discovered in this case covered a remarkable 221 days, potentially placing each Appellant at home on several dozen specific occasions, far more than the single instances discovered in Karo and Kyllo. See Kyllo, 533 U.S. at 30; Karo, 468 U.S. at 709, 714.

c.

The Supreme Court considered long-term electronic location surveillance in United States v.

Jones, 132 S. Ct. 945 (2012). In that case, the government, acting without a warrant, installed a Global Positioning System ("GPS") device on a suspect's vehicle to track the movements of the vehicle over a 28-day period. Jones, 132 S. Ct. at 948. The D.C. Circuit had decided that this practice was a search because (1) a reasonable individual would not expect that the sum of her movements over a month would be observed by a stranger in public, and (2) this information could reveal "an intimate picture" of her life not disclosed by any one of her movements viewed individually. United States v. Maynard, 615 F.3d 544, 561-64 (D.C. Cir. 2010), aff'd sub. nom. Jones, 132 S. Ct. 945.

The Supreme Court unanimously affirmed the D.C. Circuit without reaching full agreement as to the basis for this decision. See Jones, 132 S. Ct. at 954; id. at 964 (Alito, J., concurring in the judgment). The entire Court did agree however that Knotts had explicitly left unanswered the constitutionality of "dragnet type law enforcement practices" like the form of "twenty-four hour surveillance" employed in Jones. Knotts, 460 U.S. at 283-84); see Jones, 132 S. Ct. at 952 n.6 (Scalia, J., writing for the majority); id. at 956 n.* (Sotomayor, J., concurring); id. at 963 n.10 (Alito, J., concurring in the judgment). Justice Scalia's majority opinion, expressing the views of five Justices, held that the government's installation of the GPS device on the suspect's vehicle constituted a search under the traditional trespass-based theory of Fourth Amendment protection, bypassing the reasonable-expectation-of-privacy analysis established in Katz. See id. at 949-52. While acknowledging that "[s]ituations involving merely the transmission of electronic signals without

trespass would remain subject to Katz analysis," Justice Scalia declined to address this question. Id. at 953; see also id. at 954 ("It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.").

In two concurring opinions, five Justices confronted the Katz question and agreed that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Id. at 955 (Sotomayor, J., concurring); id. at 964 (Alito, J., concurring in the judgment). Justice Sotomayor echoed the D.C. Circuit's concerns about the government's ability to record an individual's movements and aggregate the information "in a manner that enables the Government to ascertain, more or less at will," private facts about the individual, such as her "political and religious beliefs, sexual habits, and so on." Id. at 956. Neither concurrence indicated how long location surveillance could occur before triggering Fourth Amendment protection, but, considering the investigation challenged in Jones, Justice Alito stated that "the line was surely crossed before the 4-week mark." Id. at 964.

The privacy interests affected by long-term GPS monitoring, as identified in Maynard and the Jones concurrences, apply with equal or greater force to historical CSLI for an extended time period. See Commonwealth v. Augustine, 4 N.E.3d 846, 861 (Mass. 2014) ("CSLI implicates the same nature of privacy concerns as a GPS tracking device."). "[C]itizens of this country largely expect the freedom

to move about in relative anonymity without the government keeping an individualized, turn-by-turn itinerary of our comings and goings." Renée McDonald Hutchins, Tied Up in Knotts? GPS Technology and the Fourth Amendment, 55 UCLA L. Rev. 409, 455 (2007). Much like long-term GPS monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life. As the D.C. Circuit stated in Maynard, "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts." 615 F.3d at 561-62; compare Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS 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."), with State v. Earls, 70 A.3d 630, 642 (N.J. 2013) ("[CSLI] can reveal not just where people go — which doctors, religious services, and stores they visit — but also the people and groups they choose to affiliate with and when they actually do so.").

Inspection of historical CSLI may provide even more private information about an individual than the locational monitoring challenged in Maynard/Jones. The surveillance at issue in that case was limited to movements of an automobile on public roads. See Jones, 132 S. Ct. at 948. Quite unlike an automobile, a cell phone is a small hand-

held device that is often hidden on the person of its user and seldom leaves her presence. As previously discussed, cell phone users regularly carry these devices into their homes and other private spaces to which automobiles have limited access at best. See Augustine, 4 N.E.3d at 861.[4] Thus, unlike GPS monitoring of a vehicle, examination of historical CSLI can permit the government to track a person's movements between public and private spaces, impacting at once her interests in both the privacy of her movements and the privacy of her home.[5]

Considering the multiple privacy interests at stake, it is not surprising that we are not the first court to recognize as objectively reasonable cell

---

[4] Cell phones are not subject to the "lesser expectation of privacy in a motor vehicle," which, as noted in Knotts, "has little capacity for escaping public scrutiny." 460 U.S. at 281 (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality)). Additionally, while a car "seldom serves . . . as the repository of personal effects[,]" id., cell phones often provide access to substantial collections of private notes and records, hiding these personal effects from inspection even while themselves hidden from view in their owners' purses or pockets, see Riley, 134 S. Ct. at 2489-91.

[5] Indeed, a recent survey by the Pew Research Center revealed that 82% of adults feel that the details of their physical location revealed by cell phone GPS tracking is at least "somewhat sensitive," with half of adults considering this information "very sensitive." Pew Research Center, Public Perceptions of Privacy and Security in the Post-Snowden Era 34 (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf (saved as ECF opinion attachment). This percentage rivals that of adults who consider their health information and the content of their phone conversations, emails, and text messages at least "somewhat sensitive" – 81%, 81%, 77%, and 75%, respectively. Id. at 32-34.

phone users' expectation of privacy in their long-term CSLI. See, e.g., Augustine, 4 N.E.3d at 865-66 (reasonable expectation of privacy in location information shown in historical CSLI records); Earls, 70 A.3d at 632 (reasonable expectation of privacy in location of cell phones); Tracey v. State, 152 So.3d 504, 526 (Fla. 2014) (objectively reasonable expectation of privacy in "location as signaled by one's cell phone"); In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 539 (D. Md. 2011) ("reasonable expectation of privacy both in [subject's] location as revealed by real-time [CSLI] and in his movement where his location is subject to continuous tracking over an extended period of time, here thirty days"); In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info. (In re Application (E.D.N.Y.)), 809 F. Supp. 2d 113, 120 (E.D.N.Y. 2011) ("reasonable expectation of privacy in long-term cell-site-location records").[6]

---

[6] As the dissenting opinion points out, a number of courts that have addressed the issue have not reached the same conclusion we reach today. Courts that have reached the opposite conclusion, like the dissent, have typically done so through application of the "third-party" doctrine as discussed in Part II.C.4 infra.

In United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), the Sixth Circuit held that the defendant "did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone." 690 F.3d at 777. This case involved locational surveillance of two cell phones in real time over the course of a few days as the users transported marijuana along public roads. Id. at 776. The Sixth Circuit determined that the case was governed by Knotts, id. at 777-78, and distinguished Jones based on the "comprehensiveness of the tracking" in that case, involving "'constant monitoring'" over

Even the Supreme Court, in Riley, specifically cited "[h]istoric location information" as among the heightened privacy concerns presented in government inspection of cell phones, as such information details the user's "specific movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2490.[7]

Taken together, Karo, Kyllo, and the views expressed in Riley and the Jones concurrences support our conclusion that the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time. Cell phone tracking through inspection of CSLI is one such technology. It is possible that the CSLI for a particular cell phone is not very revealing at all because, for instance, the phone has been turned off or it has made few or no connections to the cellular network. But the government cannot know in advance of obtaining this information how revealing it will be or whether it will detail the cell phone user's movements in private spaces. See Earls,

---

the course of four weeks, id. at 780 (quoting Jones, 132 S. Ct. at 963 (Alito, J., concurring in the judgment)). The instant case is similarly distinguishable.

[7] Some courts, including the district court in this case, as well as the dissent, have suggested that privacy interests in real-time or prospective location information are greater than those in historical location information, like that at issue in this case. See (Quartavious) Davis, 785 F.3d at 509 n.10; Graham, 846 F. Supp. 2d at 391. We see no constitutional distinction between the two types of data. A person's expectation of privacy in information about where she has been is no less reasonable, or less deserving of respect, than that regarding where she is or where she is going.

70 A.3d at 642. We hold, therefore, that the government engages in a Fourth Amendment search when it seeks to examine historical CSLI pertaining to an extended time period like 14 or 221 days.[8]

3.

The district court concluded that this case is distinguishable from Karo and Maynard/Jones because the type of locational surveillance at issue in those cases permits real-time tracking with greater precision and continuity than the examination of historical CSLI. See Graham, 846 F. Supp. 2d at 391-92, 404. The use of GPS technology challenged in Maynard/Jones permitted law enforcement to track the suspect's vehicle continuously at every moment "'24 hours a day for 28 days[,]'" id. at 392 (quoting Maynard, 615 F.3d at 558), while, here, the CSLI records only disclose a finite number of location data points for certain points in time.

This distinction is constitutionally insignificant. The Fourth Amendment challenge is directed toward the government's investigative conduct, i.e., its decision to seek and inspect CSLI records without a warrant. There is no way the government could have known before obtaining the CSLI records how granular the location data in the records would be. If Appellants had been in constant use of their phones as they moved about each waking day – constantly starting and terminating calls – then the government would have obtained a

[8] This case does not require us to draw a bright line as to how long the time period for historical CSLI can be before its inspection rises to the level of a Fourth Amendment search, and we decline to do so.

continuous stream of historical location information approaching that of GPS. A similar or greater degree of continuity would have been achieved if Appellants had smartphones that automatically connect to the nearest cell site every few minutes or seconds.

As it turns out, the CSLI records did reveal an impressive 29,659 location data points for Graham and 28,410 for Jordan, amounting to well over 100 data points for each Appellant per day on average. This quantum of data is substantial enough to provide a reasonably detailed account of Appellants' movements during the 221-day time period, including movements to and from the cell-site sectors in which their homes were located. We therefore reject the district court's suggestion that the CSLI was not sufficiently continuous to raise reasonable privacy concerns.

The district court also questioned the precision of the location data itself, concluding that the CSLI did not identify sufficiently precise locations to invade a reasonable privacy expectation. Unlike GPS data, the court found, CSLI "can only reveal the general vicinity in which a cellular phone is used." Graham, 846 F. Supp. 2d at 392.

The precision of CSLI in identifying the location of a cell phone depends in part on the size of the coverage area associated with each cell-site sector listed in the records.[9] Service providers have

[9] Sprint/Nextel's custodian testified at trial that the cell sites listed in the records each had, at most, a two-mile radius of operability. Each cell site, therefore, covered no greater than approximately 12.6 square miles, divided into three sectors of approximately 4.2 square miles or less.

begun to increase network capacity and to fill gaps in network coverage by installing low-power cells such as "microcells" and "femtocells," which cover areas as small as 40 feet.[10] The intense competition among cellular networks provides ample reason to anticipate increasing use of small cells and, as a result, CSLI of increasing precision. We must take such developments into account. See Kyllo, 533 U.S. at 36 ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.").

In any event, the CSLI at issue here was precise enough, at minimum, to support reasonable inferences about Appellants' locations at specific points in time. Otherwise, the information would have lacked any probative value at trial. The very reason that the government obtained and introduced the evidence was to establish Appellants' locations during times surrounding the charged robberies.[11]

---

[10] See Federal Communications Commission, Public Safety Tech Topic #23 – Femtocells, http://www.fcc.gov/help/public-safety-tech-topic-23-femtocells; PR Newswire, Small Cells Market 2014-2019: Femtocell, Picocell, & Microcell Prospects for LTE, SONs, Wireless Offloading & Heterogeneous Networks (Nov. 6, 2014), http://www.prnewswire.com/news-releases/small-cells-market-2014-2019-femtocell-picocell-microcell-prospects-for-lte-sons-wireless-offloading--heterogeneous-networks-281857341.html; Nancy Gohring, Femtocells Make Way Into Enterprises, ComputerWorld (May 7, 2011), http://www.computerworld.com/article/2550032/mobile-wireless/ femtocells-make-way-into-enterprises.html.

[11] Specifically, the government used the CSLI to show, among other things, that Graham was within a few miles of the Dollar Tree before and after the robbery of January 17, 2011; Graham was within a few miles of the 7-Eleven before and after the

Investigators and prosecutors must have believed, after analyzing the CSLI, that it was sufficiently precise to establish Appellants' whereabouts. The fact that inference was required to glean Appellants' past locations from the CSLI does not ameliorate or lessen in any manner the invasion of privacy. Indeed, the Supreme Court, in Kyllo, specifically rejected "the novel proposition that inference insulates a search . . . ." Id. at 36 (citing Karo, 468 U.S. 705). We therefore reject the government's argument that the CSLI was not adequately precise to infringe upon Appellants' expectations of privacy in their locations and movements.

4.

We also disagree with the district court's and the dissent's conclusion that Appellants lacked a reasonable expectation of privacy in their CSLI because the CSLI records were kept by Sprint/Nextel in the ordinary course of business. See Graham, 846 F. Supp. 2d at 403; post at 111.

The dissent argues first that "[t]he nature of the governmental activity" at issue in this case sets it apart from Karo, Kyllo, and Jones. Post at 108-09. While Karo, Kyllo, and Jones each involved direct

---

robbery of January 22, 2011; minutes after the robbery of Shell on February 1, 2011, Jordan was near the Shell and then both he and Graham were near Jordan's apartment; Appellants were both near Jordan's apartment approximately 45 minutes before robbery of Burger King on February 5, 2011; Graham was near the Burger King within minutes of the robbery; Appellants were together a few miles north of the Burger King minutes after the robbery; and Graham was near the McDonald's approximately one half hour before the McDonald's robbery.

and contemporaneous surveillance by government agents, the locational tracking challenged here was achieved through government inspection of records held by a third party.

This distinction is inconsequential. The precedents of this Court and others show that a Fourth Amendment search may certainly be achieved through an inspection of third-party records. See, e.g., Doe v. Broderick, 225 F.3d 440, 450-52 (4th Cir. 2000) (holding that detective's examination of a patient file held by a methadone clinic was a search and, without probable cause, violated the patient's Fourth Amendment rights); DeMassa v. Nunez, 770 F.2d 1505, 1508 (9th Cir. 1985) (holding that "an attorney's clients have a legitimate expectation of privacy in their client files"); cf. Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (holding that patients enjoy a reasonable expectation of privacy that the results of diagnostic tests will not be disclosed to law enforcement without the patient's consent).[12] That the government acquired Appellants'

---

[12] In the sense most crucial to a proper Fourth Amendment analysis, "[t]he nature of the governmental activity" challenged in this case, post at 108-09, was not unlike that challenged in Karo, Kyllo, and Jones. The dissent's language is apparently drawn from Smith v. Maryland, 442 U.S. 735 (1979), where the Court deemed it important to identify "the nature of the state activity that is challenged" in order to determine the precise nature of Smith's Fourth Amendment claim. 442 U.S. at 741. Specifically, this initial inquiry was made in order to determine whether Smith could claim an invasion of his property or intrusion into a constitutionally protected area, under the traditional trespass-based theory of Fourth Amendment protection. Because the challenged governmental activity was the installation of a pen register "on telephone company property at the telephone company's central offices," Smith

private information through an inspection of third-party records cannot dispose of their Fourth Amendment claim.

Yet the dissent seizes upon the fact that the government obtained Appellants' CSLI from a third-party cell service provider and maintains that we have placed our focus on the wrong question. Instead of assessing the reasonableness of Appellants' expectation of privacy in their "location and movements over time," our dissenting colleague

---

could make no such claim. Id. Instead, Smith claimed an invasion of a legitimate expectation of privacy in the numbers he dialed, which the government obtained through use of the pen register. Id. at 742.

In this sense, the nature of the governmental activity challenged in this case is not unlike the activities challenged in Karo, Kyllo, and Jones. In Karo and Kyllo, the nature of the challenged governmental activity was the use of technology to acquire certain private information rather than the physical invasion of constitutionally protected property or spaces. See Karo, 468 U.S. at 714; Kyllo, 533 U.S. at 34-35. The governmental activity challenged in Jones was of both sorts: installation of a GPS tracking device effected through a trespass onto Jones' property, and use of the device to obtain information about Jones' location and movements over an extended period of time. As previously noted, the majority confined its analysis to the trespass without considering the nature of the information the government subsequently acquired. 132 S. Ct. at 949-54. In the concurrences, five Justices focused on the government's acquisition of location information and whether this conduct invaded a legitimate expectation of privacy. Because the challenged activity in the present case, like those considered in Karo, Kyllo, and the Jones concurrences, is the government's non-trespassory acquisition of certain information, our inquiry is properly focused on the legitimacy of Appellants' expectation of privacy in this information.

would frame the question as "whether an individual has a reasonable expectation of privacy in a third party's records that permit the government to deduce this information." Post at 109. But even the analyses in the cases upon which the dissent relies focused foremost on whether, under Katz, the privacy expectations asserted for certain information obtained by the government were legitimate. See United States v. Miller, 425 U.S. 435, 442 (1976) ("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." (emphasis added)); Smith v. Maryland, 442 U.S. 735, 742 (1979) ("[P]etitioner's argument that [the] installation and use [of a pen register] constituted a 'search' necessarily rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone." (emphasis added)). In answering that question, the fact that the information at issue in Miller and Smith was contained in records held by third parties became relevant only insofar as the defendant in each case had "voluntarily conveyed" the information to the third party in the first place. See Miller, 425 U.S. at 442; Smith, 442 U.S. at 743-44.

It is clear to us, as explained below, that cell phone users do not voluntarily convey their CSLI to their service providers. The third-party doctrine of Miller and Smith is therefore inapplicable here.

a.

The Supreme Court held in Miller and Smith that "a person has no legitimate expectation of privacy in information he voluntarily turns over to

third parties." Smith, 442 U.S. at 743-44; see also Miller, 425 U.S. at 442. This is so 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." Miller, 425 U.S. at 443.[13]

In Miller, the government used defective subpoenas to obtain financial records from the defendant's bank. 425 U.S. at 436. The Court determined first that the defendant could not claim an unconstitutional invasion of his "private papers" because he had neither ownership nor possession of the transactional records at issue. Id. at 440-41 (citation omitted). Next, the Court turned to the defendant's claim that the government violated his privacy interests in the contents of the bank records. Id. at 442. Because such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," the Court held that the depositor lacks "any legitimate expectation of privacy" in this

[13] This "third-party" doctrine finds its roots in cases involving consensual disclosures to informants or undercover government agents. See United States v. White, 401 U.S. 745, 751-752 (1971); Hoffa v. United States, 385 U.S. 293, 302-303 (1966); Lopez v. United States, 373 U.S. 427, 439 (1963). White, Hoffa, Lopez, and similar cases generally establish that a person who confides information about her illegal activities in another bears the risk that this information will be reported to law enforcement, see White, 401 U.S. at 752, and introduced as evidence against her, see Lopez, 373 U.S. at 439. Any expectation she holds that this information will be held in confidence is not one entitled to Fourth Amendment protection. See White, 401 U.S. at 749; Hoffa, 385 U.S. at 301.

information. Id. at 442. "[I]n revealing his affairs to another," the defendant assumed the risk "that the information [would] be conveyed by that person to the Government." Id. at 443.

In Smith, a telephone company, at the request of police, utilized a pen register device to record the numbers dialed from the home phone of Michael Lee Smith, a man suspected of robbing a woman and then harassing her through anonymous phone calls. 442 U.S. at 737. Smith argued that the warrantless installation of the pen register was an unreasonable search. Id. at 737-38. The Court determined, first, that people generally understand that they must communicate the numbers they dial to the phone company and that the company has facilities for recording and storing this information permanently. Id. at 742. Even if Smith had an actual expectation of privacy in the numbers he dialed, this would not be a "legitimate" expectation because he "voluntarily conveyed" the numerical information to the phone company and "'exposed'" the information to the company's recording and storage equipment. Id. at 744. In so doing, Smith "assumed the risk" that the company would disclose this information to law enforcement. Id.

We recently applied the third-party doctrine of Miller and Smith in United States v. Bynum, 604 F.3d 161 (4th Cir. 2010), where the government served administrative subpoenas on a website operator to obtain a user's account information. 604 F.3d at 162. Specifically, the government obtained the user's name, email address, telephone number, and physical address, id. at 164, all information that the user entered on the website when he opened his

account, id. at 162. Citing Smith, we determined that, in "voluntarily convey[ing] all this information" to the Internet company, the user "'assumed the risk'" that this information would be revealed to law enforcement. Id. at 164 (quoting Smith, 442 U.S. at 744). The user, therefore, could not show that he had either an actual or an objectively reasonable expectation of privacy in this information. Id.

These precedents do not categorically exclude third-party records from Fourth Amendment protection. They simply hold that a person can claim no legitimate expectation of privacy in information she voluntarily conveys to a third party. It is that voluntary conveyance – not the mere fact that the information winds up in the third party's records – that demonstrates an assumption of risk of disclosure and therefore the lack of any reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone user does not "convey" CSLI to her service provider at all – voluntarily or otherwise – and therefore does not assume any risk of disclosure to law enforcement.[14]

---

[14] At the outset of its argument that the third-party doctrine applies here, the dissent insists that Appellants "exposed" their CSLI to their service provider and therefore assumed the risk of disclosure to law enforcement. Post at 111. This "exposure" language is derived from Miller and Smith, but it is clear in each of those cases that any "exposure" of the information at issue to the third party's employees or facilities occurred only through the defendant's voluntary conveyance of that information to the third party. See Miller, 425 U.S. at 442 (noting that the financial information at issue had been "voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business" (emphasis

The service provider automatically generates CSLI in response to connections made between the cell phone and the provider's network, with and without the user's active participation. See Augustine, 4 N.E.3d at 862 ("CSLI is purely a function and product of cellular telephone technology, created by the provider's system network at the time that a cellular telephone call connects to a cell site."); id. at 863 (describing CSLI as "location-identifying by-product" of cell phone technology). "Unlike the bank records in Miller or the phone numbers dialed in Smith, cell-site data is neither tangible nor visible to a cell phone user." In re Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010), vacated, 724 F.3d 600 (5th Cir. 2013). A user is not required to actively submit any location-identifying information when making a call or sending a message. Such information is rather "quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the target user." Id. at 833. We cannot impute to a cell phone user the risk that information about her location created by her service provider will be disclosed to law enforcement when she herself has not actively disclosed this information.

---

added)); Smith, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." (emphasis added)). The dissent goes on to argue that Appellants did indeed voluntarily convey the wealth of cell site location data points at issue here to their service provider by choosing generally to operate and carry their phones. We reject this contention.

Notably, the CSLI at issue in this appeal details location information not only for those transmissions in which Appellants actively participated – i.e., messages or calls they made or answered – but also for messages and calls their phones received but they did not answer. When a cell phone receives a call or message and the user does not respond, the phone's location is identified without any affirmative act by its user at all – much less, "voluntary conveyance." See In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government (In re Application (Third Circuit)), 620 F.3d 304, 317 (3d Cir. 2010) ("[W]hen a cell phone user receives a call, he hasn't voluntarily exposed anything at all."). We conclude, in agreement with the analysis of the Third Circuit in In re Application (Third Circuit) and that of several state supreme courts, that the third-party doctrine of Smith and Miller does not apply to CSLI generated by cell phone service providers. See id.; Augustine, 4 N.E.3d at 862-63; Tracey, 152 So.3d at 525; see also Earls, 70 A.3d at 641-42 (categorically rejecting third-party doctrine).

b.

The Fifth Circuit, in In re Application of U.S. for Historical Cell Site Data (In re Application (Fifth Circuit)), 724 F.3d 600 (5th Cir. 2013), and the en banc Eleventh Circuit in United States v. (Quartavious) Davis, 785 F.3d 498 (11th Cir. 2015), have reached the opposite conclusion. While acknowledging that the cell phone user "does not directly inform his service provider of the location of the nearest cell phone tower[,]" the Fifth Circuit

decided that users voluntarily convey CSLI to their service providers through general use of their cell phones. In re Application (Fifth Circuit), 724 F.3d at 614.[15] In reaching this conclusion, the court relied on the proposition, advanced by the government, that "users know that they convey information about their location to their service providers when they make a call." Id. at 612. The Eleventh Circuit followed suit, suggesting that because users are generally aware that their calls are connected through cell towers, their use of their phones amounts to voluntary conveyance of "their general location within that cell tower's range[.]" (Quartavious) Davis, 785 F.3d at 511.

We cannot accept the proposition that cell phone users volunteer to convey their location information simply by choosing to activate and use their cell phones and to carry the devices on their person. Cell phone use is not only ubiquitous in our society today but, at least for an increasing portion of our society, it has become essential to full cultural and economic participation. See Quon, 560 U.S. at 760 ("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."); Riley, 134 S. Ct. at 2484 ("[M]odern cell phones . . . are now

[15] In United States v. Guerrero, 768 F.3d 351 (5th Cir. 2014), the Fifth Circuit reaffirmed its holding in In re Application (Fifth Circuit) in affirming denial of a motion to suppress CSLI evidence. See 768 F.3d at 358-61.

such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."). People cannot be deemed to have volunteered to forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones. "The fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by 'choosing' to carry a cell phone must be rejected." In re Application (E.D.N.Y.), 809 F. Supp. 2d at 127, quoted in Tracey, 152 So.3d at 523.[16]

Users' understanding of how cellular networks generally function is beside the point. The more

---

[16] The dissent points out that similar arguments were made in dissenting opinions in Miller and Smith and ultimately rejected by the Court. We do not doubt that the financial services implicated in Miller or the telephone service implicated in Smith were any less crucial to social and economic participation than cell phone service has become. But the determination in each of those cases that the defendant had assumed the risk of disclosure to law enforcement did not rely upon the defendant's general choice to avail himself of these services. The assumption of risk was based on voluntary acts by which the defendant conveyed specific information to a third party while using these services. Smith, for instance, actively and voluntarily turned specific numbers over to his phone company, and was surely aware of what numbers he was turning over, when he placed specific calls. See Smith, 442 U.S. at 742. Smith even conceded that he could claim no legitimate expectation of privacy in the same numbers had he placed the calls through a live operator. Id. at 744. Similarly here, we do not believe that Appellants could claim a legitimate privacy expectation had they specifically identified their location or the closest cell tower to their service provider each time a transmission was made to or from their cell phones.

pertinent question is whether users are generally aware of what specific cell sites are utilized when their phones connect to a cellular network. After all, it is the specificity with which CSLI identifies cell sites that allows users' location to be tracked and raises privacy concerns. We have no reason to suppose that users generally know what cell sites transmit their communications or where those cell sites are located. A cell phone user cannot be said to "voluntarily convey" to her service provider information that she never held but was instead generated by the service provider itself without the user's involvement.[17]

Both the Fifth and Eleventh Circuits emphasized that service providers maintain CSLI records for their own business purposes rather than for law enforcement purposes and on this basis concluded that a subscriber can have no legitimate privacy expectation in the information these records contain. See In re Application (Fifth Circuit), 724 F.3d at 611-12; (Quartavious) Davis, 785 F.3d at 511-12. CSLI records are, however, wholly unlike

---

[17] In (Quartavious) Davis, the Eleventh Circuit pointed out that the pen register information at issue in Smith had the effect of disclosing precise information about the phone user's location. 724 F.3d at 511-12. Pen register information could be used to place the phone user at a specific address at a specific time "because the phone lines at issue in Smith corresponded to stationary landlines at known physical addresses." Id. The location information at issue in the present case is not "stationary" but permits tracking of a person's movements across private and public spaces. In this way, CSLI raises greater locational privacy concerns than any location information revealed through use of a stationary landline. See Karo, 468 U.S. at 715.

business records such as "credit card statements, bank statements, hotel bills, purchase orders, and billing invoices," which the government "routinely" obtains from third-party businesses by subpoena. Id. at 506. These sorts of business records merely capture voluntary commercial transactions to which the business and its individual client or customer are parties. See Miller, 425 U.S. at 442. CSLI, on the other hand, records transmissions of radio signals in which the cell phone service subscriber may or may not be an active and voluntary participant.

We agree with our sister circuits that a service provider's business interest in maintaining CSLI records is a relevant consideration in determining whether a subscriber can have a legitimate expectation of privacy in this information. But it is not the only consideration. Courts consider not only such "concepts of real or personal property law" in making this determination but also "'understandings that are recognized and permitted by society.'" Carter, 525 U.S. at 88 (citation omitted). As we have explained, society recognizes an individual's privacy interest in her movements over an extended time period as well as her movements in private spaces. The fact that a provider captures this information in its account records, without the subscriber's involvement, does not extinguish the subscriber's reasonable expectation of privacy. Applying the third-party doctrine in this context would simply permit the government to convert an individual's cell phone into a tracking device by examining the massive bank of location information retained by her service provider, and to do so without probable cause. See David Gray & Danielle Citron, The Right to Quantitative Privacy, 98 Minn. L. Rev. 62, 140 (2013)

("If the government lacks legal authority to install and monitor a GPS-enabled tracking device, then it can get the same information by securing locational data from OnStar, Lojac, a cellular phone provider, or any number of 'apps' that gather and use locational information as part of their services." (emphasis added)).

This is not a case like Hoffa, where a person assumes the risk that an associate or confidante will disclose her communications to law enforcement, see 385 U.S. at 302-03; nor is this a case like Miller, where a person assumes the risk that a bank will disclose her financial transactions to the government, see 425 U.S. at 443. Cell phone users do not actively or knowingly communicate or "trade" their location information to their service providers as part of the consideration for the services provided, to say nothing of the documentation of such information in reproducible formats. That this information winds up in the provider's hands as a consequence of how cellular networks function does not and should not affect cell phone users' reasonable expectations of privacy in this information or society's respect for that expectation.

c.

Courts have recognized that not all private information entrusted to third-party providers of communications services is subject to warrantless government inspection. As far back as 1877, the Supreme Court recognized Fourth Amendment protection against warrantless inspection of the contents of mail entrusted to the postal service for delivery. Ex parte Jackson, 96 U.S. 727, 733 (1877). In so holding, the Court recognized a distinction

between, on one hand, protected matter "intended to be kept free from inspection, such as letters[] and sealed packages[,]" and, on the other hand, unprotected matter "purposefully left in a condition to be examined" as well as the "outward form and weight" of sealed articles. Id.

The Court continued to recognize this distinction 90 years later in Katz: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." 389 U.S. at 351-52 (citations omitted). Katz involved a Fourth Amendment challenge to use of an electronic recording device attached to the outside of a public phone booth that recorded the petitioner's side of a phone conversation. Id. at 348-49. Applying the principle that the Fourth Amendment protects that which a person "seeks to preserve as private," id. at 351, the Court held that "[o]ne who occupies [a public phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world[,]" id. at 352. Although shutting the door to the phone booth proved inadequate to prevent the petitioner's private words from being overheard, and indeed would have been inadequate to prevent monitoring by the phone company, the petitioner demonstrated an expectation of privacy society would accept as reasonable. See Smith, 442 U.S. at 746-47 (Stewart, J., dissenting); Katz, 389 U.S. at 361 (Harlan, J., concurring).

In the current digital age, courts continue to accord Fourth Amendment protection to information entrusted to communications intermediaries but intended to remain private and free from inspection. Courts have, for example, deemed government inspection of the contents of emails a Fourth Amendment search but have declined to do the same for email address information used to transmit emails. Compare United States v. Warshak, 631 F.3d 266, 287-88 (6th Cir. 2010) (holding that email subscribers enjoy a reasonable expectation of privacy in the content of their emails even though such content is accessible to Internet service providers), with United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that government surveillance of a computer to discover email address information, IP addresses, and amount of data transmitted by email does not constitute a Fourth Amendment search).

The dissent argues essentially that, like the forms of address information at issue in Forrester, CSLI is simply information that facilitates the routing of communications rather than protected content, and on this basis distinguishes cases like Warshak. Post at 124. CSLI is of course more than simple routing information; it tracks a cell phone user's location across specific points in time.[18] And as

[18] The dissent argues that types of information deemed unworthy of Fourth Amendment protection "'track[]' some form of activity when aggregated over time." Post at 125. To be sure, we do not hold that a person may claim Fourth Amendment protection for records of just any type of information that happens to disclose a location, i.e., her location when she deposits an article of mail or engages in a credit card transaction. We do hold that a person may claim protection for

previously noted, cell phone users generally consider their location information no less sensitive than the contents of emails and phone calls.[19] Like a user of web-based email who intends to maintain the privacy of her messages, however, there is nothing the typical cell phone user can do to hide information about her location from her service provider.[20] In the absence of any evidence that Appellants or cell phone users generally intend for their location information to be open to inspection by others, we cannot treat the fact that CSLI is used to route communications and is recorded by intermediaries as dispositive of Appellants' claim of Fourth Amendment protection for this information.

d.

Our review of well settled Fourth Amendment jurisprudence teaches us that, even as technology evolves, protections against government intrusion should remain consistent with those privacy expectations society deems reasonable. See, e.g., United States v. U.S. Dist. Court for E. Dist. of

---

her long-term CSLI because this information may track practically all of the movements a person makes over an extended period of time. This feature sets CSLI apart from the various sorts of address and routing information cited in the dissent.

[19] See supra note 4.

[20] It seems that, here, Appellants took what little action was possible that might have concealed their personal location information from their service provider. Graham's service was subscribed in his wife's name, and Jordan used an alias or proxy on his account, although the record does not indicate that these actions were taken specifically to protect Appellants' privacy interests.

Mich., S. Div., 407 U.S. 297, 312 (1972) ("There is, understandably, a deep-seated uneasiness and apprehension that [government's capability for electronic surveillance] will be used to intrude upon cherished privacy of law-abiding citizens."); Berger v. State of N.Y., 388 U.S. 41, 62 (1967) ("'[T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual; . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments . . . .'") (quoting Lopez, 373 U.S. at 1389 (Warren, C.J., concurring in the result)). That is not to say that societal expectations of privacy cannot change over time, but the advent of new technology alone – even major technological advances – is not a sufficient basis upon which to infer an equally dramatic shift in people's privacy expectations.[21]

---

[21] In Smith, for instance, the Supreme Court rejected the notion that different constitutional rules should apply to different technological means of engaging in the same form of communication, lest "a crazy quilt" be made of the Fourth Amendment. 442 U.S. at 745. Just as a caller could claim no legitimate expectation of privacy in telephone connections made personally by an operator, Smith could claim no privacy expectation in numbers he dialed to connect his calls through the phone company's automatic switching equipment. Id. at 744. Smith, in this way, reflects the principle that the use of new technology to hide from view what would otherwise be exposed cannot by itself expand Fourth Amendment rights where none would otherwise exist.

The natural corollary to this principle is that a technological advance alone cannot constrict Fourth Amendment protection for private matters that would otherwise be hidden or inaccessible. Confronting the question of "what limits there are upon [the] power of technology to shrink the realm of

It turns out that the proliferation of cellular networks has left service providers with a continuing stream of increasingly precise information about the locations and movements of network users. Prior to this development, people generally had no cause for concern that their movements could be tracked to this extent. That new technology has happened to generate and permit retention of this information cannot by itself displace our reasonable privacy expectations; nor can it justify inspection of this information by the government in the absence of judicially determined probable cause.

Courts and commentators have for years begun to acknowledge the increasing tension, wrought by our technological age, between the third-party doctrine and the primacy Fourth Amendment doctrine grants our society's expectations of privacy. In her concurring opinion in Jones, Justice Sotomayor declared the assumption that people lack reasonable privacy expectations in information held by third parties "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

---

guaranteed privacy" in Kyllo, 533 U.S. at 34, Justice Scalia concluded for the majority that the use of new technology "to explore details of the home that would previously have been unknowable without physical intrusion" constitutes a search, id. at 40. "This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Id. at 34. As one prominent commentator explained, the Fourth Amendment not only "permit[s] access to that which technology hides" but also "protect[s] that which technology exposes." Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 580 (2009).

out mundane tasks." Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

It is concerning that now, during a time and context in which the viability of the third-party doctrine, "the Lochner of search and seizure law," Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 563 (2009) (footnote omitted), has never been in graver doubt, the dissent's treatment of the doctrine would expand it into a full-on exception to the legitimate-expectation-of-privacy inquiry. Post at 133. Our dissenting colleague reads into Miller and Smith a rule that would preclude virtually any Fourth Amendment challenge against government inspection of third-party records. But just a few years ago, writing for the Court in Bynum, our dissenting colleague rightly declared that the question of whether an individual has a reasonable expectation of privacy in a matter searched is "[t]he 'touchstone' of Fourth Amendment analysis[.]" 604 F.3d 164 (citation omitted). Contrary to her current views, the third-party doctrine was not devised to side-step this question; rather, the doctrine aids the court precisely in deciding whether certain privacy expectations are reasonable by societal standards. See Smith, 442 U.S. at 743-44; Bynum, 604 F.3d at 164; (Quartavious) Davis, 785 F.3d at 527 (Rosenbaum, J., concurring) ("Supreme Court precedent fairly may be read to suggest that the third-party doctrine must be subordinate to expectations of privacy that society has historically recognized as reasonable."). Smith and Miller do not endorse blind application of the doctrine in cases where information in which there are clearly reasonable privacy expectations is generated and recorded by a third party through an accident of

technology. The third-party doctrine is intended to delimit Fourth Amendment protections where privacy claims are not reasonable - not to diminish Fourth Amendment protections where new technology provides new means for acquiring private information. See Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 527 (2011) ("[I]f a new technology permits the government to access information that it previously could not access without a warrant, using techniques not regulated under preexisting rules that predate that technology, the effect will be that the Fourth Amendment matters less and less over time.").

* * * * *

For these reasons, we decline to apply the third-party doctrine here and hold that Appellants have a reasonable expectation of privacy in their long-term CSLI.[22] Specifically, we conclude that the

---

[22] Echoing the sentiments of the Fifth and Eleventh Circuits, the dissent suggests that any privacy concerns raised by the government's warrantless acquisition of CSLI should be presented to Congress and addressed legislatively, rather than to the courts for constitutional protection. Post at 131-33. We think the same argument might be made in any case in which a new technological means or investigative practice is employed to obtain personal information and the court must decide the Katz question. In each of these cases, the court is tasked with making an assessment of what privacy interests society might deem reasonable. This is a task for which one might argue the legislative branch is suited, but one that is, as a matter of constitutional interpretation, nonetheless imposed upon the courts. See Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803) ("It is emphatically the province and duty of the judicial department to say what the law is.").

government's procurement and inspection of Appellants' historical CSLI was a search, and the government violated Appellants' Fourth Amendment rights by engaging in this search without first securing a judicial warrant based on probable cause.[23] If the Twenty-First Century Fourth Amendment is to be a shrunken one, as the dissent proposes, we should leave that solemn task to our superiors in the majestic building on First Street and not presume to complete the task ourselves.

D.

Although we conclude that the government violated Appellants' Fourth Amendment rights in procuring their CSLI without a warrant based on probable cause, the records were not subject to suppression because the government acted in good-faith reliance on court orders issued under the SCA.

"The exclusionary rule 'generally prohibits the introduction at criminal trial of evidence obtained in violation of a defendant's Fourth Amendment rights[.]'" United States v. Stephens, 764 F.3d 327, 335 (4th Cir. 2014) (quoting Pa. Bd. of Prob. & Parole

[23] Moving beyond her theoretical objections to our holding, our dissenting colleague declares the holding "bizarre in practice," citing the fact that the cell service records admitted in this case included not just CSLI but also information we have not deemed Fourth Amendment protected. Post at 126. The § 2703(d) orders in this case specifically requested the CSLI associated with Appellants' cell service accounts. After today's holding, the government will need to secure a warrant for this information. This requirement would not affect whether, in response to such a warrant, the service provider produces records that include information for which a warrant is not specifically required. It is unclear to us what makes this practice "bizarre."

v. Scott, 524 U.S. 357, 359 (1998)). But our system of justice and society at large incur "'heavy costs'" when courts are required to disregard reliable evidence, "'suppress the truth'" about criminal conduct, and release to the community a criminal who might otherwise be subject to imprisonment. Id. (quoting (Willie Gene) Davis v. United States, 131 S. Ct. 2419, 2427 (2011)). Considering that the "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations[,]" (Willie Gene) Davis, 131 S. Ct. at 2426, courts apply the rule to exclude evidence only where the benefits of deterrence outweigh the costs of suppression, id. at 2427.

In assessing the deterrent value of suppression, our focus is properly placed on culpable police conduct and not on the actions of legislators and judicial officers. Id. at 2432-33. Where law enforcement acts "with an objectively 'reasonable good-faith belief' that their conduct is lawful," there is no need for deterrence sufficient to justify the exclusion of reliable evidence. Id. at 2427 (quoting United States v. Leon, 468 U.S. 897, 909 (1984)). This good-faith exception to the exclusionary rule applies where law enforcement reasonably relies on (1) an enacted statute, unless that statute is clearly unconstitutional, Illinois v. Krull, 480 U.S. 340, 349-50 (1987); (2) a search warrant or other court order issued by a neutral magistrate, unless issuance of the order is clearly defective, Leon, 468 U.S. at 922-23, 926; or (3) "binding appellate precedent," (Willie Gene) Davis, 131 S. Ct. at 2429.

Here, the government is entitled to the good-faith exception because, in seeking Appellants' CSLI, the government relied on the procedures established

in the SCA and on two court orders issued by magistrate judges in accordance with the SCA. The government's first § 2703(d) application requested data regarding calls and messages to and from Appellants' phones during four time periods and described robberies under investigation that occurred during some of those time periods. After learning about other similar robberies, the government submitted a second application to request records for the much broader 221-day time frame. The second application included the same facts provided in the first application but added descriptions of additional robberies under investigation. Appellants do not claim that the government was "dishonest or reckless" in preparing either application. Leon, 468 U.S. at 926. Upon consideration of each of the government's applications, two magistrate judges of the district court respectively issued § 2703(d) orders to Sprint/Nextel for the disclosure of Appellants' account records. There is nothing in the record to suggest that either magistrate "abandoned" her or his "detached and neutral" role such that a well trained officer's reliance on either order would have been unreasonable. Id.

Appellants do not attack the facial validity of the § 2703(d) orders. Instead, they argue that the government cannot reasonably rely on the § 2703 orders because, in offering law enforcement a choice between seeking a warrant and a § 2703(d) court order to obtain subscriber records, the statute is internally inconsistent. Appellants point out that, while a warrant requires a showing of probable cause, a § 2703(d) order requires a significantly

lesser showing – a standard akin to reasonable suspicion.[24]

We find no "inherent contradiction on the face of the SCA." Appellants' Br. 46. Section 2703(c) unambiguously offers law enforcement a choice between specific avenues to obtain records from service providers. "Unless a statute is clearly unconstitutional, an officer cannot be expected to question the judgment of the legislature that passed the law." Krull, 480 U.S. at 349-50. That the statute provides options that set different requirements on law enforcement does not amount to a contradiction or render the statute facially unconstitutional.

Appellants argue next that the SCA cannot justify the government's unconstitutional use of discretion granted under the statute to seek a § 2703(d) court order instead of a warrant for historical CSLI. Citing State v. Thompson, 810 P.2d 415 (Utah 1991), Appellants argue that the good-faith exception is inapplicable where a prosecutor fails to exercise a statutory grant of discretionary power within constitutional bounds. In a related case prior to

---

[24] Appellants cite In re Application (Third Circuit), wherein the Third Circuit reviewed a district court's denial of § 2703(d) applications for CSLI. 620 F.3d at 305-06. In seeking to determine whether a magistrate has authority under the statute to deny an application that satisfies the requirements of § 2703(d), the court stated, "There is an inherent contradiction in the statute or at least an underlying omission." Id. at 319. The court did not specifically identify any contradiction in the statute. We presume that the court's comment is based on the statute's lack of clarity as to the scope of the magistrate's discretion to grant or deny § 2703(d) applications. That does not appear to be the "inherent contradiction" upon which Appellants rely.

Thompson, the Supreme Court of Utah had determined that issuance and use of certain subpoenas by the state attorney general under Utah's Subpoena Powers Act violated the Utah Constitution in several respects for which the attorney general was responsible. In re Criminal Investigation, 7th Dist. Ct. No. CS-1, 754 P.2d 633, 658-59 (Utah 1988), cited in Thompson, 810 P.2d at 146. In Thompson, the court determined that "a good faith exception [to Utah's exclusionary rule] . . . would be inapplicable to illegal subpoenas issued . . . by the attorney general, who is chargeable for the illegality[,]" and therefore evidence obtained through use of the illegal subpoenas was subject to suppression. 810 P.2d at 420. The constitutional defects in the issuance and use of the subpoenas were clear enough for the attorney general to concede that the Subpoena Powers Act had been unconstitutionally applied. See id. at 639, 658.

The constitutionally infirm decision of the prosecution in the present case to seek § 2703(d) orders instead of warrants was not so clear, at least not prior to today's decision. Prior to our ruling today, neither this Court nor the U.S. Supreme Court had deemed the government's conduct in this case unconstitutional.

We agree with Appellants that, when in doubt, the government should "err on the side of constitutional behavior[.]" Leon, 468 U.S. at 926 (Brennan, J., dissenting). And we recognize that, at the time the government obtained the CSLI at issue here, court rulings outside of this Circuit were in conflict as to the constitutionality of obtaining this information without a warrant. But the government's

conduct in this case was not governed by disagreements among a handful of courts outside this Circuit, and there was no decisional authority in this Circuit suggesting that the choice presented in § 2703(c) was unconstitutional as applied to CSLI from cell phone service providers. We conclude, therefore, that the government reasonably relied on the SCA in exercising its option to seek a § 2703(d) order rather than a warrant. The good-faith exception applies.[25] We affirm denial of Appellants' motion to suppress.

III.

Appellants appeal the district court's admission of certain testimony of Jeff Strohm, records custodian for Sprint/Nextel, and Special Agent Colin Simons of the FBI, arguing that portions constitute expert testimony in the guise of lay opinion.

As previously stated, we review the district court's evidentiary rulings for abuse of discretion. United States v. Johnson, 617 F.3d 286, 292 (4th Cir. 2010). "A district court has abused its discretion if its decision 'is guided by erroneous legal principles' or 'rests upon a clearly erroneous factual finding.'" Morris v. Wachovia Sec., Inc., 448 F.3d 268, 277 (4th Cir. 2006) (quoting Westberry v. Gislaved Gummi AB, 178 F.3d 257, 261 (4th Cir. 1999)). If we find such an abuse of discretion, we review it under the

[25] Now that we have determined that law enforcement violates the Fourth Amendment when it acts without a warrant to obtain an individual's long-term CSLI, its choice under § 2703(c) is constrained. The government may no longer rely on the statute to justify an election not to secure a warrant for this information.

harmless-error standard stated in Rule 52(a) of the Federal Rules of Criminal Procedure. Johnson, 617 F.3d at 292. We find the district court's error harmless if we can "say with fair assurance, after pondering all that happened without stripping the erroneous action from the whole, that the judgment was not substantially swayed by the error." Id. (quoting United States v. Brooks, 111 F.3d 365, 371 (4th Cir. 1997)) (internal quotation marks omitted).

For the reasons explained below, we find no abuse of discretion in the district court's admission of Simons' testimony and portions of Strohm's testimony. Insofar as the court erred in admitting other portions of Strohm's testimony as that of a lay witness, we find such error harmless.

A.

The admission of expert testimony is governed by Rule 702 of the Federal Rules of Evidence, which permits one "who is qualified as an expert" to offer at trial opinion testimony based on "scientific, technical, or other specialized knowledge." Prior to admitting any expert testimony, the trial judge must act as a gatekeeper, conducting a preliminary assessment of whether the expert's proffered testimony is both relevant and reliable. Kumho Tire Co. v. Carmichael, 526 U.S. 137, 149 (1999) (citing Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579, 592 (1993)).

Under Rule 701, lay witnesses are "'not permit[ted] . . . to express an opinion as to matters which are beyond the realm of common experience and which require the special skill and knowledge of an expert witness.'" Certain Underwriters at Lloyd's, London v. Sinkovich, 232 F.3d 200, 203 (4th Cir.

2000) (quoting Randolph v. Collectramatic, Inc., 590 F.2d 844, 846 (10th Cir. 1979)). "At bottom, . . . Rule 701 forbids the admission of expert testimony dressed in lay witness clothing, but it 'does not interdict all inference drawing by lay witnesses.'" United States v. Perkins, 470 F.3d 150, 156 (4th Cir. 2006) (quoting United States v. Santos, 201 F.3d 953, 963 (7th Cir. 2000)).

B.

Appellants challenge Strohm's testimony regarding how cell phones connect with cell sites and the operations and radio frequency range of cell sites. Strohm testified that, in seeking or receiving a connection to the cellular network, a cell phone connects to the cell tower emitting the strongest signal, and that cell sites in urban areas have a two-mile maximum range of connectivity. He testified further that, aside from proximity, factors such as line of sight and volume of call traffic may affect the ability of a particular cell tower to connect to a phone, but, in any case, the phone must be located within two miles of any cell tower in the Baltimore area in order to connect to it.

Strohm's testimony that signal strength determines which cell tower will connect to a phone and that cell towers in urban areas have a two-mile maximum range of operability was not opinion testimony. These statements were not conclusions Strohm drew based on any specialized reasoning or assessment, and were not presented in the form of an opinion or inference. They were facts based on Strohm's experience as an employee of Sprint/Nextel. Indeed, at trial, defense counsel specifically declined to challenge Strohm's testimony that a cell phone

connects to the tower emitting the strongest signal. Strohm's testimony as to cell sites' range of operability required no greater than the same minimal technical knowledge. The district court did not abuse its discretion in admitting this testimony by a lay witness.

Similarly, Strohm's testimony that factors including proximity, line of sight, and call traffic may affect a phone's ability to connect to a particular cell tower did not rise to the level of an expert opinion. Strohm did not, for instance, engage in any analysis comparing the factors or seek to determine how these factors resulted in any particular connection, which would have required scientific, technical, or specialized knowledge. He merely presented the fact that these factors exist, which prevented the jury from being misled into believing that signal strength is a matter of proximity alone or that a cell phone will always connect to the nearest tower.

Even if the district court abused its discretion in admitting Strohm's testimony about these factors, any such error was harmless. The government's evidence as to the locations of Appellants' cell phones at various points in time was based solely on the locations of the cell towers listed in Sprint/Nextel's records and each tower's two-mile maximum range of operability. In order for Appellants' cell phones to connect to the towers listed in Sprint/Nextel's records, they had to have been located within two miles of the listed towers, even if line of sight or call traffic affected which cell sites within two miles ultimately connected to the phones. The mere fact that these factors exist, therefore, could not have

substantially affected the jury's assessment of the government's evidence and the resultant verdict.

The admission of other aspects of Strohm's lay testimony is more concerning. Strohm provided explanations of how cell phones connect to a cellular network for the completion of calls, going, at times, into technical details about operations performed by cell sites and how calls are routed through network switches. Such testimony was clearly "based on scientific, technical, or specialized knowledge within the scope of Rule 702." Fed. R. Evid. 701(c); see also United States v. Yeley-Davis, 632 F.3d 673, 684 (10th Cir. 2011) ("The agent's testimony concerning how cell phone towers operate constituted expert testimony because it involved specialized knowledge not readily accessible to any ordinary person."); United States v. Evans, 892 F. Supp. 2d 949, 954 (N.D. Ill. 2012) (holding that testimony as to "how cellular networks operate, i.e., the process by which a cell phone connects to a given tower" requires an expert qualified to "meet the demands of Rule 702 and Daubert").

We conclude, however, that any error in the admission of this testimony was harmless. The technical aspects of how cell phone calls are completed have little to do with establishing the location of a cell phone based on cell site information. All that really matters is that the cell site had a particular range of connectivity and that the phone connected to a cell site at a particular time – facts established through Sprint/Nextel's records and admissible portions of Strohm's testimony.

C.

Appellants challenge testimony offered by Agent Simons regarding his creation of maps based on the CSLI disclosed by Sprint/Nextel. The maps plot the locations of certain cell sites listed in the CSLI records, the business establishments robbed, and Jordan's apartment. The maps also identify the dates and times of inbound and outbound calls made by Appellants' phones through the plotted cell sites.

Simons' testimony did not amount to an expert opinion. To create the maps, Simons utilized mapping software that was marketed to the general public and required little more than identification of the various locations he intended to plot. He entered the locations of the businesses and Jordan's apartment by their physical addresses and the cell sites by latitude and longitude, as disclosed by Sprint/Nextel. The minimal technical knowledge or skill required to complete this task was not so "specialized" as to constitute a matter of expertise within the meaning of Rule 702. See United States v. Henderson, 564 F. App'x 352, 364 (10th Cir. 2014) (unpublished) (holding that agent's testimony regarding review of cell phone records and creation of map of cell tower locations "did not require expertise"). The district court did not abuse its discretion in admitting Simons' testimony.

IV.

Jordan appeals the district court's decision to set certain restrictions on his testimony, arguing that these restrictions infringed upon his constitutional right to testify in his own defense. We review the district court's evidentiary rulings for abuse of

discretion but review constitutional questions de novo. United States v. Dinkins, 691 F.3d 358, 382 (4th Cir. 2012). We find no constitutional error or abuse of discretion in the challenged restrictions.

A.

A criminal defendant has a constitutional right to testify on her own behalf derived from the compulsory process clause of the Sixth Amendment and the due process clause of the Fourteenth Amendment. Rock v. Arkansas, 483 U.S. 44, 52 (1987); United States v. Midgett, 342 F.3d 321, 325 (4th Cir. 2003). The right to testify is not absolute, however, and "'may, in appropriate cases, bow to accommodate other legitimate interests in the criminal trial process.'" Rock, 483 U.S. at 55 (quoting Chambers v. Mississippi, 410 U.S. 284, 295 (1973)). This Court has previously held, for instance, that "criminal defendants do not have a right to present evidence that the district court, in its discretion, deems irrelevant or immaterial." United States v. Prince-Oyibo, 320 F.3d 494, 501 (4th Cir. 2003); see also Taylor v. Illinois, 484 U.S. 400, 410 (1988) (holding that compulsory process clause does not give defendant "an unfettered right to offer testimony that is incompetent, privileged, or otherwise inadmissible under standard rules of evidence"); Montana v. Egelhoff, 518 U.S. 37, 42 (1996) (applying same rule in due process context).

The defendant exercising her right to testify "must comply with established rules of procedure and evidence designed to assure both fairness and reliability in the ascertainment of guilt and innocence." Chambers, 410 U.S. at 302. Thus, under Rule 403 of the Federal Rules of Evidence, even

relevant testimony by the defendant "may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury[.]"

B.

The district court set certain restrictions on Jordan's testimony to prevent unfair prejudice to Graham. Specifically, Jordan was precluded from [REDACTED].

Jordan did not object to these restrictions at trial, so any error committed by the district court in imposing the restrictions is subject to plain-error review. United States v. Godwin, 272 F.3d 659, 672 (4th Cir. 2001); see also Fed. R. Crim. P. 52(b). We will reverse only upon a showing by Jordan that an error by the district court was "clear or obvious[,]" affected Jordan's substantial rights, and "'seriously affect[s] the fairness, integrity or public reputation of judicial proceedings.'" Godwin, 272 F.3d at 672-73 (quoting United States v. Olano, 507 U.S. 725, 732 (1993)).

C.

We find no constitutional error in the restrictions the district court placed on Jordan's testimony because the restrictions did not prevent Jordan from presenting a full narrative in his defense. Jordan was permitted to testify – and did indeed testify – as follows: In late January or early February of 2011, Graham and a group of friends began coming to Jordan's home on a regular basis. Jordan would socialize with them "for a little while" before asking them to leave because "I don't live like they live[.]" J.A. 2303. Friends of Graham were at

Jordan's apartment on the morning of February 5, 2011, and Graham arrived later. After Jordan and Graham visited a liquor store together, Graham dropped Jordan off at his home, and then Jordan went to visit his aunt's home on the 300 block of North Stricker Street in Baltimore. Graham came through the neighborhood, and Jordan arranged for him to meet an unidentified person to "do their little business." J.A. 2310. When Graham returned to Jordan, he asked Jordan to take him to a Wal-Mart store to purchase a television set. Jordan drove Graham's truck and was eventually stopped by police, and the two were arrested. When asked about the weapons recovered from his home after his arrest, Jordan testified that he did not know how they got there but believed that Graham's friends left them there.[26]

Jordan argues that the court's restrictions prevented him from explaining the basis of his association with Graham. He avers that a full account of his relationship with Graham would have shown that they were together and communicated at certain times for reasons other than to commit robberies. The only alternative explanation disclosed in Jordan's brief is that [REDACTED]. Jordan also sought to testify that, [REDACTED].

The restrictions imposed by the district court were not arbitrary but were appropriately tailored to suit their purpose in preventing unfair prejudice to

---

[26] Specifically, Jordan stated, "I think the day I let his home boys stay [in my house], they left them in there." J.A. 2314. Viewed in context, the statement implicitly referred to Graham. The court admonished Jordan for this statement, instructing him "to confine [his] remarks to what [he] did." Id.

Graham. Testimony that had the potential to prejudice Graham while bearing no real exculpatory value for Jordan. Specifically naming Graham and his associates would have had minimal probative value in Jordan's favor. The district court did not abuse its discretion in determining that the risk of unfair prejudice to Graham outweighed the probative value of any of this testimony. See Fed. R. Evid. 403.

D.

Jordan argues that testimony about [REDACTED] would have explained a prior inconsistent statement the government used to impeach him.

[REDACTED] The cell phone records obtained by the government disproved this verion of events, showing that the last call Graham made to Jordan was much earlier that afternoon and then both Jordan's and Graham's phones were near each other, but several miles away from Jordan's apartment.

Jordan's initial version of events also contradicted his testimony at trial, wherein he stated that Graham picked him up from Stricker Street to ask for a ride – not from his home. When confronted by the inconsistent statement made to authorities, Jordan admitted that he had lied, but stated that he did so because he was "scared." J.A. 2314, 2343. Jordan avers that his initial account was not accurate because he was afraid to inform the authorities about [REDACTED]. However, Jordan was precluded from explaining the basis for his fear at trial due to the court's restriction against testifying about [REDACTED]. During its closing argument, the government disputed whether

Jordan's purported fear was the reason for the lies he told authorities, stating to the jury, "he didn't mislead the police because he was afraid. He misled the police to get away with what he had done." J.A. 2444.

We agree with Jordan that, in the context of the government's efforts to impeach him, it was an abuse of discretion for the court to prevent Jordan from rebutting these efforts through a full explanation of his prior inconsistent statement. Jordan's counsel, however, did not object to the restriction and thus forfeited the issue. The forfeited error only warrants reversal if it was "clear or obvious" and affected Jordan's substantial rights. Godwin, 272 F.3d at 672. Absent an objection that would have brought the issue to the district court's attention, the court's abuse of discretion was not "clear or obvious."

Further, Jordan fails to show that the error affected his substantial rights. At trial, the government introduced substantial evidence tending to disprove Jordan's version of events. Such evidence included data from test drives and Computer Aided Dispatch ("CAD") reports showing that it would not have been possible for Graham to have picked Jordan up from the 300 block of North Stricker Street during the brief time period between the McDonald's robbery and the point at which Jordan and Graham were apprehended by Baltimore police. On this record, we cannot conclude that the government's impeachment of Jordan by prior inconsistent statement was necessary for the jury to determine that Jordan's version of events was untrue.

In sum, Jordan fails to show that the restriction against testimony about [REDACTED] on the date of the Burger King and McDonald's robberies was plain error.[27] We affirm.

V.

Jordan appeals the district court's denial of his motion for severance, arguing that the joint trial of him and Graham compromised his right to testify fully in his own defense. "We review a district court's denial of a motion for severance for an abuse of discretion." United States v. Lighty, 616 F.3d 321, 348 (4th Cir. 2010) (citation omitted). The district court has "broad discretion" to deny a motion for severance. Id. To establish abuse of discretion, "a defendant must show that he was prejudiced by the denial of a severance motion . . . ." Id. (citation omitted).

---

[27] Based on the apparent agreement between Jordan's counsel, the government, and the district court about the restrictions on Jordan's testimony, the government argues that Jordan waived the issue and that even plain-error review is not warranted. See Olano, 507 U.S. at 733 ("Waiver is different from forfeiture. Whereas forfeiture is the failure to make the timely assertion of a right, waiver is the 'intentional relinquishment or abandonment of a known right.'") (citation omitted). Jordan argues that the restriction implicated his personal constitutional right to testify in his own defense, which cannot be waived by defense counsel or the court. United States v. Flores-Martinez, 677 F.3d 699, 711 (5th Cir. 2012); United States v. Teague, 953 F.2d 1525, 1532 (11th Cir. 1992); see also Midgett, 342 F.3d at 327 (agreement between court and defense counsel did not effect waiver of defendant's constitutional right to testify). We need not decide whether Jordan waived the issue because there is no plain error.

Under Rule 8(b) of the Federal Rules of Criminal Procedure, multiple defendants "may be charged in the same indictment if they are alleged to have 'participated in the same act or transaction, or in the same series of acts or transactions, constituting an offense or offenses.'" Id. (quoting Fed. R. Crim. P. 8(b)). "There is a preference in the federal system for joint trials of defendants who are indicted together[]" because such trials "promote efficiency and 'serve the interests of justice by avoiding the scandal and inequity of inconsistent verdicts.'" Zafiro v. United States, 506 U.S. 534, 537 (1993) (quoting Richardson v. Marsh, 481 U.S. 200, 210 (1987)). "Accordingly, severance under Rule 14 is only warranted when 'there is a serious risk that a joint trial would compromise a specific trial right of one of the defendants, or prevent the jury from making a reliable judgment about guilt or innocence.'" United States v. Najjar, 300 F.3d 466, 473 (4th Cir. 2002) (quoting Zafiro, 506 U.S. at 539). The defendant seeking severance must show "'that actual prejudice would result from a joint trial, . . . and not merely that a separate trial would offer a better chance of acquittal.'" Id. (quoting United States v. Reavis, 48 F.3d 763, 767 (4th Cir. 1995)).

Jordan argues that the joint trial compromised his right to provide exculpatory testimony on his own behalf and resulted in prejudice to him. As discussed in Part IV supra, the district court placed some restrictions on Jordan's testimony to prevent prejudice to Graham and to permit a fair joint trial between the defendants. Jordan contends, again, that these restrictions impaired his right to provide testimony that would exculpate him but tend to inculpate Graham. This Court has previously held,

however, that a defendant's "desire . . . to exculpate himself by inculpating another [is] insufficient grounds to require separate trials." Najjar, 300 F.3d at 474 (quoting United States v. Spitler, 800 F.2d 1267, 1271 (4th Cir. 1986)). As explained in Part IV, Jordan was permitted to present a full narrative in his defense to the charges against him. The testimony that Jordan sought to provide inculpating Graham held little exculpatory value for Jordan. The restrictions did not prejudice Jordan and did not prevent the jury from making a reliable judgment.

As we stated in Najjar,

> [Rule 14] requires more than finger pointing. There must be such a stark contrast presented by the defenses that the jury is presented with the proposition that to believe the core of one defense it must disbelieve the core of the other . . . or "that the jury will unjustifiably infer that this conflict alone demonstrates that both are guilty."

Id. (citations omitted).

In summary, Graham's defense was that he was not any of the individuals seen in video surveillance of the armed robberies charged in the case; witnesses' identifications of Graham were dubious; the CSLI in the cell phone records was imprecise; the government failed to show that Graham's and Jordan's association amounted to an agreement to commit crime; and items of clothing and the vehicle used to link Graham to various robberies were common and not distinctive.

Similarly, Jordan contended at trial that he did not drive Graham's pickup truck to flee any robbery; that he was visiting a relative's home when the Burger King and McDonald's robberies occurred; that descriptions of individuals who committed the Shell robbery did not match Jordan; that the government failed to show that his association with Graham amounted to a conspiracy; and that the CSLI was imprecise. Additionally, Jordan asserted in his defense that he did not sanction Graham's friends using his apartment to store weapons and clothing. There is little, if any, contrast between Appellants' defenses, and certainly no contrast so stark as to necessitate severance. We cannot conclude that the district court abused its broad discretion and therefore affirm denial of Jordan's motion for severance.

VI.

Jordan challenges the district court's decision to exclude from evidence two out-of-court statements of an unavailable declarant, i.e., Graham. We review the district court's decision for abuse of discretion. United States v. Bumpass, 60 F.3d 1099, 1102 (4th Cir. 1995).

Hearsay is generally not admissible in evidence, Fed. R. Evid. 802, given the "dangers" of insincerity, misperception, misremembrance, and ambiguity presented in out-of-court statements, Williamson v. United States, 512 U.S. 594, 598 (1994). Rule 804(b)(3), however, provides an exception to the hearsay rule for statements made against the declarant's interest, including statements that, at the time they were made, "had so great a

tendency . . . to expose the declarant to civil or criminal liability" that a reasonable person in her position would not have made the statements unless believing them to be true. Fed. R. Evid. 804(b)(3). "[H]earsay may be admitted under this exception if (1) the declarant is unavailable, (2) the statement is genuinely adverse to the declarant's penal interest, and (3) 'corroborating circumstances clearly indicate the trustworthiness of the statement.'" Bumpass, 60 F.3d at 1102. Satisfying these requirements presents a "formidable burden" to the party offering the statement. Id.

Jordan argues that the district court should have admitted a written statement bearing the signature "Aaron Graham" and the recording of a jail call between Graham and an individual called Tony. Dated February 9, 2011, the written statement reads, "I Aaron Graham I did pick up Eric Jordan 10-15 minutes prior to my truck being pulled over and he had no knowledge of anything I'm accused of." J.A. 2638. On the jail call, Tony asks, "Remember, didn't you write a statement or something saying he wasn't with you or something like that?" Graham responds, "Oh, yeah, yeah, yeah, yeah, yeah." J.A. 2218. Exercising his Fifth Amendment right not to testify at trial, Graham was unavailable to testify as the declarant of the statements at issue. See United States v. Dargan, 738 F.3d 643, 649 (4th Cir. 2013).

We conclude that the district court did not abuse its discretion in excluding the statements from evidence. First, the written statement was not genuinely adverse to Graham's penal interest. The statement admits of no wrongdoing by Graham but

rather casts the charges against Graham as mere allegations.

Second, Jordan fails to show corroborating circumstances that clearly indicate that the written statement is trustworthy. While recognizing that "the precise nature of the corroboration required by Rule 804(b)(3) cannot be fully described," this Court has identified several factors that courts consider in "determining whether sufficient corroboration exists to justify admitting a statement under the rule[.]" Bumpass, 60 F.3d at 1102. These factors include

> (1) whether the declarant had at the time of making the statement pled guilty or was still exposed to prosecution for making the statement, (2) the declarant's motive in making the statement and whether there was a reason for the declarant to lie, (3) whether the declarant repeated the statement and did so consistently, (4) the party or parties to whom the statement was made, (5) the relationship of the declarant with the accused, and (6) the nature and strength of independent evidence relevant to the conduct in question.

Id.

The fact that Graham and Jordan were friends or associates likely gave Graham a motive to exonerate Jordan and a reason to lie for this purpose. Further, there is no indication in the record that the content of the written statement was ever repeated by Graham; nor is there any independent evidence,

aside from Jordan's own testimony, to show that Jordan was not with Graham during the robberies. Graham was facing prosecution on the date attached to the written statement, but he could not have exposed himself to greater criminal liability or risk of conviction in making the statement, given its non-incriminating character.

In sum, we agree with the district court that there are not sufficient corroborating circumstances to "clearly" indicate the trustworthiness of the written statement. We find no abuse of discretion in the district court's decision to exclude the hearsay statement.

We also agree with the district court that the jail call is insufficient to establish that the written statement was indeed a statement by Graham. See Fed. R. Evid. 901. On the call, Graham appears to affirm that he, at some point, wrote a statement, but his comment falls short of identifying or otherwise authenticating the written statement Jordan sought to admit into evidence. We find no abuse of discretion in the district court's decision to exclude jail call as non-relevant. See Fed. R. Evid. 401.

VII.

Jordan challenges the district court's denial of his motion to suppress evidence obtained in searches of his home conducted after his arrest in February 2011. The searches were conducted pursuant to two warrants Jordan argues were invalid based on defects in the affidavit of probable cause submitted to obtain the first warrant and in the return after the first warrant was executed. Jordan does not dispute that the affidavits for both warrants provided a

substantial basis for a finding of probable cause. Instead, Jordan argues that the warrants were invalid because (1) the affidavit supporting the first warrant omitted exculpatory information while including information about robberies for which Jordan was not ultimately charged; and (2) the affiant falsely certified in the return that he executed the warrant. We find no reversible error.

A.

Jordan identifies two sets of defects in the affidavit supporting the first warrant: (1) it included facts about the robberies of January 22, 2011, with which Jordan was not ultimately charged; and (2) it omitted the facts about these robberies that would tend to exculpate Jordan, including the fact that descriptions of the robbers did not match Jordan and the lack of forensic evidence linked to Jordan. Jordan claims that he was prejudiced by these additions and omissions.

An affidavit supporting a search warrant is entitled to "a presumption of validity[,]" Franks v. Delaware, 438 U.S. 154, 171 (1978), but a defendant may "attack a facially sufficient affidavit" "in certain narrowly defined circumstances[,]" United States v. Colkley, 899 F.2d 297, 300 (4th Cir. 1990) (citing Franks, 438 U.S. 154). After making a preliminary showing, a defendant may demand under the Fourth Amendment a hearing to determine (1) whether an affiant has "knowingly and intentionally, or with reckless disregard for the truth," included a false statement in a warrant affidavit; and (2) whether the false statement "is necessary to the finding of probable cause[.]" Franks, 438 U.S. at 155-56.

"[T]he search warrant must be voided" if perjury or reckless disregard is established by a preponderance of the evidence, and, "with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause[.]" Id. at 156. In such a case, "the fruits of the search [must be] excluded to the same extent as if probable cause was lacking on the face of the affidavit." Id. This rule "also applies when affiants omit material facts 'with the intent to make, or in reckless disregard of whether they thereby made, the affidavit misleading.'" Colkley, 899 F.2d at 300 (quoting United States v. Reivich, 793 F.2d 957, 961 (8th Cir. 1986)).

Jordan did not request a Franks hearing before the district court and has made no showing before this Court that the affiant on the challenged affidavit included any false statement, whether "knowingly and intentionally, . . . with reckless disregard for the truth," or otherwise. Franks, 438 U.S. at 155. Jordan also has not shown that any of the complained-of statements included in the affidavit were "necessary to the finding of probable cause" or that any of the excluded facts would have prevented a finding of probable cause. Id. at 156.

We also reject Jordan's challenge with respect to the potentially exculpatory information he complains was not included in the first warrant affidavit. In Colkley, this Court affirmed denial of a defendant's motion to suppress fruits of an arrest warrant that "did not contain certain potentially exculpatory information known to the affiant." 899 F.2d at 298. The defendant "made no showing that the affiant intended to mislead the magistrate by

omitting information, and because the warrant with the omitted information would in any event have been supported by probable cause . . . ." Id. Similarly here, Jordan has not shown that the affiant intended to mislead the magistrate by omitting, or was reckless in omitting, information that tended to exculpate Jordan as to the robberies of January 22, 2011.

We find no reason to set aside our presumption that the challenged warrant affidavit was valid and therefore find no reversible error in the district court's decision to admit evidence seized during the searches of Jordan's home.

B.

Citing Rule 41(f)(1) of the Federal Rules of Criminal Procedure, Jordan next argues that the first search warrant was defective because the affiant, Detective Woerner, falsely certified in the return that he executed the warrant. Rule 41(f)(1) provides that "[a]n officer present during the execution of the warrant must prepare and verify an inventory of any property seized" and that "[t]he officer executing the warrant must promptly return it — together with a copy of the inventory — to the magistrate judge designated on the warrant."

By its own terms, however, Rule 41 applies only to federal search warrants requested by "a federal law enforcement officer" or "an attorney for the government[.]" Fed. R. Crim. P. 41. This Court has held that "a warrant proceeding must meet the particulars of Rule 41 only where the warrant application was made at the direction or urging of a federal officer." United States v. Clyburn, 24 F.3d

613, 616 (4th Cir. 1994) (citations and internal quotation marks omitted). We have also held that "[n]on-constitutional violations of Rule 41 warrant suppression only when the defendant is prejudiced by the violation . . . or when 'there is evidence of intentional and deliberate disregard of a provision in the Rule[.]'" United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) (citations omitted).

The warrants Jordan challenges were prepared and executed by local law enforcement officers, not federal agents. Thus, any defect in the return cannot serve as a basis for suppression. Even if Rule 41 applied, however, Jordan has not shown that the officers intentionally or deliberately disregarded the requirements of Rule 41(f) or that he was prejudiced by the defect in the return. In this context, prejudice would be established by a showing that the search would not have taken place the same way if the officers had complied with the Rule with respect to the return. See United States v. Pangburn, 983 F.2d 449, 455 (2d Cir. 1993) ("[T]here was no prejudice to Salcido because the search of his storage locker would have taken place in exactly the same way if Rule 41 had been followed with regard to notice of the entry . . . ."). Jordan has made no such showing. The false certification of the return provides no basis for suppression in this case. We affirm the district court's decision to admit the challenged evidence.

VIII.

Jordan appeals the district court's denial of his motion for acquittal with respect to the charges for conspiracy, Hobbs Act robbery, and brandishing a

firearm during a crime of violence in connection with the Shell, Burger King, and McDonald's robberies. Rule 29(a) of the Federal Rules of Criminal Procedure requires the district court to "enter a judgment of acquittal of any offense for which the evidence is insufficient to sustain a conviction." At the close of government's case-in-chief, Jordan submitted motions for acquittal as to all offenses charged in the indictment. The district court granted the motion as to the charge under 18 U.S.C. § 922(g)(1) in Count One for being a felon in possession of a firearm but denied the motion as to the remaining counts. The jury ultimately returned guilty verdicts as to each of these offenses. Jordan argues that the evidence presented at trial was not sufficient to support the guilty verdicts beyond a reasonable doubt. We disagree.

A.

We review challenges to the sufficiency of evidence de novo. United States v. Engle, 676 F.3d 405, 419 (4th Cir. 2012), cert. denied, 133 S. Ct. 179 (2012). The Court must sustain the verdict if, "viewing the evidence and the reasonable inferences to be drawn therefrom in the light most favorable to the Government, '. . . the evidence adduced at trial could support any rational determination of guilty beyond a reasonable doubt.'" United States v. Burgos, 94 F.3d 849, 863 (4th Cir. 1996) (quoting United States v. Powell, 469 U.S. 57, 67 (1984)). In assessing the challenge, we focus on "'the complete picture that the evidence presents[,]' . . . consider[ing] the evidence 'in cumulative context' rather than 'in a piecemeal fashion[.]'" United States v. Strayhorn, 743 F.3d 917, 921-22 (4th Cir. 2014),

cert. denied, 134 S. Ct. 2689 (2014) (quoting Burgos, 94 F.3d at 863).

This Court "may not overturn a substantially supported verdict merely because it finds the verdict unpalatable or determines that another, reasonable verdict would be preferable." Burgos, 94 F.3d at 862. Rather, "reversal for insufficiency [is] '. . . confined to cases where the prosecution's failure is clear[.]'" Engle, 676 F.3d at 419 (quoting Burks v. United States, 437 U.S. 1, 17 (1978)). A defendant asserting a sufficiency challenge therefore bears a "'heavy burden[.]'" Id. (quoting United States v. Hoyte, 51 F.3d 1239, 1245 (4th Cir. 1995)).

B.

The evidence presented at trial included the following:

Three individuals were seen on video surveillance using firearms to rob Shell on February 1, 2011. Clothing matching that worn by one of the individuals, who the government sought to prove was Graham, and weapons matching those seen in the video and described by victims were later recovered from different locations inside Jordan's apartment, among his personal belongings. Photographs showed that distinctive clothing Jordan wore at the time of his arrest closely resembled that worn by a masked robber seen in the video of the Shell robbery, which was confirmed in the testimony of two police detectives. CSLI in cell phone records showed that, minutes after the Shell robbery on February 1, 2011, Jordan was near Shell and then both he and Graham were near Jordan's apartment.

Cell phone records also showed that numerous calls were made between Jordan and Graham between February 1 and February 5, 2011. CSLI showed that, on February 5, 2011, Jordan and Graham were both near Jordan's apartment approximately 45 minutes before the Burger King robbery and that Graham was near Burger King within minutes of the robbery. On that date, according to eyewitness testimony, an individual later identified as Graham used a black pistol with a white handle to rob Burger King and then McDonald's. Graham was seen fleeing each robbery by entering the passenger side of a dark colored Ford F-150 pickup truck that was driven by another individual.

Officer Corcoran testified that, during his investigation of the Burger King robbery, he received reports describing the robber, his weapon, and the getaway vehicle. A 911 call was placed reporting the McDonald's robbery and described the getaway vehicle as a pickup truck. CAD reports confirm that approximately five minutes after the call, Corcoran spotted a speeding F-150 truck on the road and saw that the passenger wore a jacket matching the description of the Burger King robber. Corcoran pursued the vehicle and activated the siren on his patrol car. The driver of the truck, who turned out to be Jordan, responded by driving up on a sidewalk before becoming trapped between heavy traffic, a construction barrier, and a moving train in front of the truck. Jordan was initially non-compliant with instructions given by Officer Corcoran but was eventually secured and arrested. Graham was arrested from the passenger side of the vehicle.

Bundles of folded and crumbled cash were recovered from Jordan and Graham, including more than $200 recovered from Jordan's person and $83 stuffed in the console inside the truck. A .25 caliber Taurus pistol with a pearl handle was found under the passenger seat of the truck and matched the description of the gun used in the Burger King and McDonald's robberies. The truck was owned by Graham and matched the description of the truck used as the getaway vehicle after each of the Burger King and McDonald's robberies. A fingerprint belonging to Graham was found at Burger King after the robbery.

Test drives were conducted of the route between McDonald's and the location on North Stricker Street where Jordan testified that he was picked up by Graham on February 5, 2011. The tests showed that the trip would take more than seven minutes to travel at the highest possible rate of speed in traffic, using emergency lights and sirens. This evidence tended to show that it would not have been possible for Jordan to have been picked up from North Stricker Street between the time of the McDonald's robbery and the pursuit by Officer Corcoran.

In addition to the foregoing evidence, the parties stipulated that the businesses robbed operated in interstate commerce and that the robberies affected interstate commerce.

Viewed as a whole and in the light most favorable to the government, a reasonable juror could accept the evidence presented at trial "as adequate and sufficient to support a conclusion of guilt beyond

a reasonable doubt[]" on each of the offenses of which Jordan was convicted. Engle, 676 F.3d at 419.

C.

Jordan's sufficiency challenges as to his robbery and firearm convictions proceed from assumptions that he was found guilty of these offenses solely on a theory of having aided and abetted armed robberies principally committed by Graham. These assumptions are dubious, considering that the jury found Jordan guilty of conspiracy in Count Four.

To prove conspiracy, the government must show "(1) an agreement between two or more people to commit a crime, and (2) an overt act in furtherance of the conspiracy." United States v. Ellis, 121 F.3d 908, 922 (4th Cir. 1997). "The existence of a 'tacit or mutual understanding' between conspirators is sufficient evidence of a conspiratorial agreement." Id. (quoting United States v. Chorman, 910 F.2d 102, 109 (4th Cir. 1990)). Such an agreement may be established through circumstantial evidence, such as the defendant's "'relationship with other members of the conspiracy, the length of this association, [the defendant's] attitude [and] conduct, and the nature of the conspiracy.'" Burgos, 94 F.3d at 858 (4th Cir. 1996) (citation omitted).

"Like the conspirators' agreement, a defendant's participation in the conspiracy 'need not be explicit; it may be inferred from circumstantial evidence.'" Id. This Court has held that "once a conspiracy is established, even a slight connection between a defendant and the conspiracy is sufficient

to include him in the plan." Ellis, 121 F.3d at 922 (internal quotation marks and citation omitted).

A reasonable fact finder could conclude from the evidence presented at trial that Jordan conspired with Graham to commit armed robberies of Shell, Burger King, and McDonald's. Circumstantial and direct evidence showing that Jordan and Graham cooperated in performing the armed robbery of Shell reflects a "'tacit and mutual understanding'" between the two and supports a reasonable inference that they had an agreement to commit this crime. Ellis, 121 F.3d at 922 (citation omitted). Evidence of the pair's involvement in the Shell robbery, ongoing communications between Jordan and Graham over the course of the days to follow, and Jordan's role as getaway driver after Graham's robberies of Burger King and McDonald's provide circumstantial evidence that Jordan and Graham agreed to cooperate in assuming their respective roles in these robberies. In sum, the evidence presented at trial was sufficient to support Jordan's conspiracy conviction.

As a co-conspirator with Graham in the Shell, Burger King, and McDonald's robberies, Jordan is liable for Graham's reasonably foreseeable acts in furtherance of the conspiracy. See United States v. Ashley, 606 F.3d 135, 142-43 (4th Cir. 2010) (citing Pinkerton v. United States, 328 U.S. 640, 647 (1946)). Jordan does not dispute that the government presented substantial evidence that Graham was responsible for Hobbs Act robbery of Shell, Burger King, and McDonald's, and used a firearm in each of

those robberies.[28] We hold, therefore, that Jordan's convictions for Hobbs Act robbery and brandishing a firearm under 18 U.S.C. § 924(c) are supported by substantial evidence.

D.

Jordan contends that the district court made a ruling that the government failed to prove Jordan's knowledge that Graham brought a firearm into the pickup truck after the McDonald's robbery. Without such evidence, Jordan argues, there was not sufficient evidence to convict him on the Hobbs Act robbery and firearm offenses arising from the Burger King and McDonald's robberies. The record discloses no clear ruling from the district court as to any evidence of Jordan's knowledge about the Taurus pistol in the truck.

Jordan directs our attention to the district court's decision to grant Jordan's Rule 29(a) motion for acquittal on Count One, which charged Jordan with being a felon in possession of a firearm under 18 U.S.C. § 922(g)(1). Liability under § 922(g)(1) may arise from a felon's voluntary and intentional possession of a firearm, whether the felon possessed the weapon actually or constructively, exclusively or

---

[28] A conviction under the Hobbs Act requires proof

> (1) that the defendant coerced the victim to part with property; (2) that the coercion occurred through the "wrongful use of actual or threatened force, violence or fear or under color of official right"; and (3) that the coercion occurred in such a way as to affect adversely interstate commerce.

United States v. Buffey, 899 F.2d 1402, 1403 (4th Cir. 1990) (citation omitted); see also 18 U.S.C. § 1951.

jointly with others. See United States v. Gallimore, 247 F.3d 134, 136-37 (4th Cir. 2001). "'Constructive possession' . . . occurs when a person 'exercise[s], or ha[s] the power to exercise, dominion and control over [an] item' of property." United States v. Scott, 424 F.3d 431, 435 (4th Cir. 2005) (quoting United States v. Shorter, 328 F.3d 167, 172 (4th Cir. 2003)). The government may "prove constructive possession of an item in instances when a defendant has dominion and control over the premises or vehicle where the item is located." Id. at 435 n.*.

The government asserted multiple theories of the felon-in-possession charge against Jordan, including the theory that Jordan was in constructive possession of the Taurus pistol through operation of the truck in which it was located. The district court rejected each of the government's theories. As to the constructive-possession theory, the district court stated two grounds for its decision: (1) "all of the evidence introduced to date indicates the firearm was under the complete individual control of the co-defendant Graham[;]" and (2) there was "no evidence tending to show that Jordan's alleged constructive possession of the firearm was voluntary as required by the Scott case." J.A. 2213.

We are not persuaded that, in so ruling, the district court implied that there was insufficient evidence that Jordan knew about the gun Graham brought into the truck. Cf. Schneckloth v. Bustamonte, 412 U.S. 218, 224 (1973) ("[Voluntariness] cannot be taken literally to mean a 'knowing' choice."). From the larger context of the court's colloquy with counsel regarding the felon-in-possession charge, it is apparent that the court's

skepticism of the constructive-possession theory was based on the view that Jordan, as "the alleged getaway driver," J.A. 2192, could not have assumed joint possession of a weapon that was solely within the control of Graham simply because Graham chose to bring it into the vehicle. In that sense, any possession Jordan had of the weapon by virtue of his control of the vehicle was not "voluntary." But that does not mean that Jordan was unaware that the weapon was present.[29]

In any case, our review of the district court's sufficiency determination is de novo, and we hold that there was indeed sufficient evidence that Jordan knew the Taurus pistol was in the truck after the Burger King and McDonald's robberies. Accordingly, we reject Jordan's sufficiency challenge to his convictions for these robberies and associated firearm offenses.

IX.

For the foregoing reasons, Appellants' Motion to Strike the Sur-Reply of the United States is granted, and the judgment of the district court is

AFFIRMED.

---

[29] We decline to reach the question of whether the district court expressed the correct view of constructive possession of a firearm through control of the vehicle in which it is located.

THACKER, Circuit Judge, concurring:

I am in agreement with Judge Davis's conclusion that cell site location information ("CSLI") cannot be obtained without a warrant but that, in this case, admission of the CSLI evidence must be sustained pursuant to the "good faith" exception to the warrant requirement. I write separately to express my concern about the erosion of privacy in this era of rapid technological development.

The tension between the right to privacy and emerging technology, particularly as it relates to cell phones, impacts all Americans. Indeed, as the Supreme Court noted in Riley v. California, cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." 134 S. Ct. 2473, 2484 (2014). Nearly every American adult owns a cell phone.[*] See Mobile Technology Fact Sheet, Pew Research Ctr., http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet (last visited July 23, 2015) (saved as ECF opinion attachment) (reporting that, as of January 2014, "90% of American adults own a cell phone"). More than three-fifths of American adults own a smartphone. See Aaron Smith, Pew Research Ctr., U.S. Smartphone Use in 2015 2 (2015), http://www.pewinternet.org/files/2015/03/PI_Smartphones_0401151.pdf (saved as ECF opinion

[*] Cell phone ownership is even higher among young adults. See Aaron Smith, How Americans Use Text Messaging, Pew Research Ctr., http://www.pewinternet.org/2011/09/19/how-americans-use-text-messaging (last visited July 23, 2015) (saved as ECF opinion attachment) (reporting that 95% of 18 to 24 year olds own a cell phone).

attachment) (reporting that "64% of American adults now own a smartphone of some kind"). And each year more Americans decide to rely solely on cell phones, untethering from landlines. See, e.g., Stephen J. Blumberg & Julian V. Luke, U.S. Dept. of Health & Human Res., Wireless Substitution: Early Release Estimates from the National; Health Interview Survey, July - December 2014 (2015), http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201506.pdf (saved as ECF opinion attachment). As of 2014, almost half of American homes only had cell phones. See id. ("More than two in every five American homes (45.4%) had only wireless telephones (also known as cellular telephones, cell phones, or mobile phones) during the second half of 2014 . . . .").

And cell phones are far more than sophisticated walkie-talkies. Unlike a walkie-talkie, which merely facilities a conversation, "a cell phone collects in one place many distinct types of information . . . that reveal much more in combination than any isolated record" or conversation. Riley, 134 S. Ct. at 2489. This information -- stored on the phone and on remote servers -- makes reconstructing a day in the life of any individual a simple task. See, e.g., id. ("The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions . . . ."). In fact, gathering and storing 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," including in the privacy of his or her own home. Id. at 2490. This is the reality of modern life.

"The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought." Id. at 2495 (2014).

It is particularly disturbing that any one of us can be tracked from afar regardless of whether or not we are actively using our phones. Even just sitting at home alone, your phone may be relaying data, including your location data. This data is transmitted to the remote servers of your service provider, where the data is stored. According to the Government, it does not need a warrant to force your service provider to turn over this information. By doing nothing, you disclosed your location information to a third party. Per the Government's theory, in so doing you have foregone your right to privacy such that a warrant is not necessary. I cannot approve of such a process (or lack thereof).

As the march of technological progress continues to advance upon our zone of privacy, each step forward should be met with considered judgment that errs on the side of protecting privacy and accounts for the practical realities of modern life.

At bottom, this decision continues a time-honored American tradition -- obtaining a warrant is the rule, not the exception.

DIANA GRIBBON MOTZ, Circuit Judge, dissenting in part and concurring in the judgment:

I concur in the judgment affirming Defendants' convictions and sentences. But, with respect, I dissent from the holding that the government violated Defendants' Fourth Amendment rights. The majority concludes that the government did so when it obtained, pursuant to 18 U.S.C. § 2703(d) court orders, but without warrants, records of the cell phone towers Defendants used to make and receive calls and text messages. That holding flies in the face of the Supreme Court's well-established third-party doctrine.[1]

The Court has long held that an individual enjoys "no legitimate expectation of privacy," and so no Fourth Amendment protection, in information he "voluntarily turns over to [a] third part[y]." Smith v. Maryland, 442 U.S. 735, 743-44 (1979). This rule applies even when "the information is revealed," as it assertedly was here, "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976). Accordingly, the government's acquisition of historical cell site location information (CSLI) from

[1] Given the majority's affirmance of Defendants' convictions on alternate grounds, its rejection of the third-party doctrine makes no difference to the result in this case. But the majority's disavowal of the third-party doctrine will have profound consequences in future cases in the Fourth Circuit. For unlike in cases arising in every other circuit to consider the matter, the government will have to obtain a search warrant supported by probable cause before obtaining even historical CSLI in this circuit.

Defendants' cell phone provider did not implicate, much less violate, the Fourth Amendment.

I.

The Fourth Amendment ensures that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Broadly, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001).

In assessing whether such a search occurred, "it is important to begin by specifying precisely the nature of the state activity that is challenged." Smith, 442 U.S. at 741 (emphasis added). Here, that "activity" is the government's acquisition from a phone company, Sprint/Nextel, of CSLI records -- i.e., the records the phone company created that identify which cell towers it used to route Defendants' calls and messages. The government did not surreptitiously view, listen to, record, or in any other way engage in direct surveillance of Defendants to obtain this information. Rather, it was Sprint/Nextel alone that obtained the information, and generated the business records, that Defendants now claim are constitutionally protected.

The nature of the governmental activity here thus critically distinguishes this case from those on which the majority relies -- cases in which the government did surreptitiously collect private

information.[2] In United States v. Karo, 468 U.S. 705, 714-15 (1984), for instance, the Drug Enforcement Agency placed a beeper within a can of ether and received tracking information from the beeper while the can was inside a private residence. Similarly, in Kyllo, 533 U.S. at 34-35, the Department of the Interior used a thermal imager to gather "information regarding the interior of the home." And in United States v. Jones, 132 S. Ct. 945, 949 (2012), the FBI and local law enforcement secretly installed a GPS tracking device on a suspect's vehicle and monitored the vehicle's movements for four weeks.

---

[2] My colleagues acknowledge this distinction but dismiss it as "inconsequential." I cannot agree. It matters, for Fourth Amendment purposes, how the government acquires information. Just as the Supreme Court applies a different analysis depending on whether the government engages in a physical trespass, see United States v. Jones, 132 S. Ct. 945, 949-53 (2012), so too the Court applies a different analysis, in non-trespassory cases, depending on whether the information at issue was voluntarily disclosed to a third party. See Smith, 442 U.S. at 743-44. Perhaps, in accord with the two lower court cases the majority cites, the Court will someday conclude that, given long-established statutory and common-law protections, the third-party doctrine does not apply to information a patient reveals to a doctor or a client to a lawyer -- i.e., that the patient and client do have reasonable expectations of privacy in information conveyed in the course of these confidential relationships. But see 1 Wayne R. LaFave, Search & Seizure: A Treatise on the Fourth Amendment § 2.7(d) (5th ed. 2012 & Supp. 2014). Clearly, however, the Court has already declined to recognize any reasonable expectation of privacy for information a phone company customer provides to the phone company. See Smith, 442 U.S. at 743-44.

On the basis of these cases, the majority contends that "the government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time." Perhaps. But that question is not before us. The question we must answer is not whether, in the abstract, an individual has a reasonable expectation of privacy in his location and movements over time. Rather, the question before us is whether an individual has a reasonable expectation of privacy in a third party's records that permit the government to deduce this information. Karo, Kyllo, and Jones, all of which involve direct government surveillance, tell us nothing about the answer to that question.

Instead, the cases that establish the third-party doctrine provide the answer. Under the third-party doctrine, an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party. Smith, 442 U.S. at 743-44. The Supreme Court has reasoned that, by "revealing his affairs to another," an individual "takes the risk . . . that the information will be conveyed by that person to the Government." Miller, 425 U.S. at 443. The Fourth Amendment does not protect information voluntarily disclosed to a third party because even a subjective expectation of privacy in such information is "not one that society is prepared to recognize as 'reasonable.'" Smith, 442 U.S. at 743 (internal quotation marks and citation omitted). The government therefore does not engage in a Fourth Amendment "search" when it acquires such information from a third party.

Applying the third-party doctrine to the facts of this case, I would hold that Defendants did not have a reasonable expectation of privacy in the CSLI recorded by Sprint/Nextel. The Supreme Court's reasoning in Smith controls. There, the defendant challenged the government's use of a pen register -- a device that could record the outgoing phone numbers dialed from his home telephone. Id. at 737. The Court held that the defendant could "claim no legitimate expectation of privacy" in the numbers he had dialed because he had "voluntarily conveyed" those numbers to the phone company by "'expos[ing]' that information to" the phone company's "equipment in the ordinary course of business." Id. at 744. The defendant thereby "assumed the risk that the company would reveal to police the numbers he dialed." Id.

Here, as in Smith, Defendants unquestionably "exposed" the information at issue to the phone company's "equipment in the ordinary course of business." Id. Each time Defendants made or received a call, or sent or received a text message -- activities well within the "ordinary course" of cell phone ownership -- Sprint/Nextel generated a record of the cell towers used. The CSLI that Sprint/Nexel recorded was necessary to route Defendants' cell phone calls and texts, just as the dialed numbers recorded by the pen register in Smith were necessary to route the defendant's landline calls. Having "exposed" the CSLI to Sprint/Nextel, Defendants here, like the defendant in Smith, "assumed the risk" that the phone company would disclose their information to the government. Id. at 744. For these reasons, the government's acquisition of that information (historical CSLI) pursuant to § 2703(d)

orders, rather than warrants, did not violate the Fourth Amendment.

Three other federal appellate courts have considered the Fourth Amendment question before us. Not one has adopted the majority's holding. Two of our sister courts have expressly held, as I would, that individuals do not have a reasonable expectation of privacy in historical CSLI records that the government obtains from cell phone service providers through a § 2703(d) order. See United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc) (holding defendant had no "objective[ly] reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls"); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (In re Application (Fifth Circuit)) (holding the government can use "[s]ection 2703(d) orders to obtain historical cell site information" without implicating the Fourth Amendment (emphasis omitted)). And although the third court opined that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way," it held that "CSLI from cell phone calls is obtainable under a § 2703(d) order," which "does not require the traditional probable cause determination" necessary for 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, 620 F.3d 304, 313, 317 (3d Cir. 2010) (In re Application (Third Circuit)).

Even in the absence of binding circuit precedent, the vast majority of federal district court

judges have reached the same conclusion.[3] Given this near unanimity of federal authority, the majority is forced to rest its holding on three inapposite state cases and three district court opinions -- including one that has been vacated, In re Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010), vacated, 724 F.3d 600 (5th Cir. 2013), and another that involves only prospective

---

[3] See, e.g., United States v. Epstein, No. 14-287, 2015 WL 1646838, at *4 (D.N.J. Apr. 14, 2015) (Wolfson, J.); United States v. Dorsey, No. 14-328, 2015 WL 847395, at *8 (C.D. Cal. Feb. 23, 2015) (Snyder, J.); United States v. Lang, No. 14-390, 2015 WL 327338, at *3-4 (N.D. Ill. Jan. 23, 2015) (St. Eve, J.); United States v. Shah, No. 13-328, 2015 WL 72118, at *7-9 (E.D.N.C. Jan. 6, 2015) (Flanagan, J.); United States v. Martinez, No. 13-3560, 2014 WL 5480686, at *3-5 (S.D. Cal. Oct. 28, 2014) (Hayes, J.); United States v. Rogers, No. 13-952, 2014 WL 5152543, at *3-4 (N.D. Ill. Oct. 9, 2014) (Kocoras, J.); United States v. Giddins, 57 F. Supp. 3d 481, 491-94 (D. Md. 2014) (Quarles, J.); United States v. Banks, 52 F. Supp. 3d 1201, 1204-06 (D. Kan. 2014) (Crabtree, J.); United States v. Serrano, No. 13-0058, 2014 WL 2696569, at *6-7 (S.D.N.Y. June 10, 2014) (Forrest, J.); United States v. Moreno-Nevarez, No. 13-0841, 2013 WL 5631017, at *1-2 (S.D. Cal. Oct. 2, 2013) (Benitez, J.); United States v. Rigmaiden, No. 08-814, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013) (Campbell, J.); United States v. Gordon, No. 09-153-02, 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012) (Urbina, J.); United States v. Benford, No. 09-86, 2010 WL 1266507, at *2-3 (N.D. Ind. Mar. 26, 2010) (Moody, J.); In re Application of the U.S. for an Order Authorizing the Disclosure of Cell Site Location Info., No. 08-6038, 2009 WL 8231744, at *9-11 (E.D. Ky. Apr. 17, 2009) (Wier, Mag. J.); In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F. Supp. 2d 76, 79-82 (D. Mass. 2007) (Stearns, J.). But see United States v. Cooper, No. 13-00693, 2015 WL 881578, at *6-8 (N.D. Cal. Mar. 2, 2015) (Illston, J.); In re Application of U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 120-27 (E.D.N.Y. 2011) (Garaufis, J.).

and real-time CSLI, In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 535 & n.4 (D. Md. 2011).[4]

In sum, the majority's holding lacks support from all relevant authority and places us in conflict with the Supreme Court and three other federal appellate courts.

II.

Despite the lack of support for its position, the majority insists that the third-party doctrine does not apply here. The majority maintains that "a cell phone user does not 'convey' CSLI to her service provider at all –- voluntarily or otherwise –- and

---

[4] Two of the state cases do not even interpret the Fourth Amendment, but instead rely on broader state constitutional protections. See Commonwealth v. Augustine, 4 N.E.3d 846, 858 (Mass. 2014) (finding "no need to wade into the[] Fourth Amendment waters" when the court could rely on article 14 of the Massachusetts Declaration of Rights); State v. Earls, 70 A.3d 630, 641-42 (N.J. 2013) (explaining that New Jersey has "departed" from Smith and Miller and does not recognize the third-party doctrine). And the court in the third state case repeatedly pointed out that it was not considering "historical cell site location records" -- like those at issue here -- but "real time cell site location information," which had been obtained, not through a § 2703(d) order, but under an order that had authorized only a "pen register" and "trap and trace device." Tracey v. State, 152 So. 3d 504, 506-08, 515-16, 526 (Fla. 2014). Thus, contrary to my colleagues' charge, it is not the dissent, but rather cases on which the majority relies, that "have suggested" that there are different privacy interests in "real-time" versus "historical" location information. See id.; see also In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 535-39 (D. Md. 2011).

therefore does not assume any risk of disclosure to law enforcement." This is the analytical lynchpin of my colleagues' holding.[5] By my count, they invoke a cell phone user's asserted lack of "voluntariness" no less than twenty times in their discussion of the third-party doctrine. But my colleagues' holding that cell phone users do not voluntarily convey CSLI misapprehends the nature of CSLI, attempts to redefine the third-party doctrine, and rests on a long-rejected factual argument and the constitutional protection afforded a communication's content.

A.

With respect to the nature of CSLI, there can be little question that cell phone users "convey" CSLI to their service providers. After all, if they do not, then who does? Perhaps the majority believes that because a service provider generates a record of CSLI, the provider just conveys CSLI to itself. But

---

[5] My colleagues also emphasize the general "sensitiv[ity]" of location information. But to the extent they do so to argue that the third-party doctrine does not apply to CSLI, they are mistaken. The third-party doctrine clearly covers information regarded as comparably "sensitive" to location information, like financial records, Miller, 425 U.S. at 442, and phone records, Smith, 442 U.S. at 745. Indeed, the public polling study the majority twice cites in attempting to establish the "sensitivity" of CSLI relates that a similar number of adults regard the phone numbers they call to be just as "sensitive" as location data. Pew Research Ctr., Public Perceptions of Privacy and Security in the Post-Snowden Era 34-35 (2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsof Privacy_111214.pdf. This is so even though the location data that the study asked about (GPS) is far more precise than the CSLI at issue here. See id. at 34.

before the provider can create such a record, it must receive information indicating that a cell phone user is relying on a particular cell tower. The provider only receives that information when a cell phone user's phone exchanges signals with the nearest available cell tower. A cell phone user therefore "conveys" the location of the cell towers his phone connects with whenever he uses the provider's network.

There is similarly little question that cell phone users convey CSLI to their service providers "voluntarily." 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."). This is so, as the Fifth Circuit explained, even though a cell phone user "does not directly inform his service provider of the location of the nearest cell phone tower." In re Application (Fifth Circuit), 724 F.3d at 614.

Logic compels this conclusion. When an individual purchases a cell phone and chooses a service provider, he expects the provider will, at a minimum, place outgoing calls, send text messages, and route incoming calls and messages. As most cell phone users know all too well, however, proximity to a cell tower is necessary to complete these tasks. Anyone who has stepped outside to "get a signal," or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters. See id. at 613 ("Cell phone users recognize that, if their phone cannot pick up a signal (or 'has no bars'), they are out of the range of their service provider's network of towers.").

A cell phone user thus voluntarily enters an arrangement with his service provider in which he knows that he must maintain proximity to the provider's cell towers in order for his phone to function. Whenever he expects his phone to work, he is thus permitting -- indeed, requesting -- his service provider to establish a connection between his phone and a nearby cell tower. A cell phone user therefore voluntarily conveys the information necessary for his service provider to identify the CSLI for his calls and texts. And whether the service provider actually "elects to make a . . . record" of this information "does not . . . make any constitutional difference." Smith, 442 U.S. at 745.

To be sure, some cell phone users may not recognize, in the moment, that they are "conveying" CSLI to their service provider. See In re Application (Third Circuit), 620 F.3d at 317. But the Supreme Court's use of the word "voluntarily" in Smith and Miller does not require contemporaneous recognition of every detail an individual conveys to a third party.[6] Rather, these cases make clear that the third-

[6] If it were otherwise, as my colleagues appear to believe, then courts would frequently need to parse business records for indicia of what an individual knew he conveyed to a third party. For example, when a person hands his credit card to the cashier at a grocery store, he may not pause to consider that he is also "conveying" to his credit card company the date and time of his purchase or the store's street address. But he would hardly be able to use that as an excuse to claim an expectation of privacy if those pieces of information appear in the credit card company's resulting records of the transaction. Cf. United States v. Phibbs, 999 F.2d 1053, 1077-78 (6th Cir. 1993) (Defendant "did not have both an actual and a justifiable privacy interest in . . . his credit card statements.").

party doctrine does not apply when an individual involuntarily conveys information -- as when the government conducts surreptitious surveillance or when a third party steals private information.

Thus, this would be a different case if Sprint/Nextel had misused its access to Defendants' phones and secretly recorded, at the government's behest, information unnecessary to the provision of cell service. Defendants did not assume that risk when they made calls or sent messages. But like the defendant in Smith, 442 U.S. at 747, Defendants here did "assume the risk" that the phone company would make a record of the information necessary to accomplish the very tasks they paid the phone company to perform. They cannot now protest that providing this essential information was involuntary.

B.

To justify its rejection of the third-party doctrine, the majority attempts to redefine it. The majority maintains that the third-party doctrine does not apply to CSLI because a cell phone user need not "actively submit any location-identifying information when making a call or sending a message." My colleagues apparently believe that an individual only "voluntarily convey[s]" information he "actively submit[s]," but such a rule is nowhere to be found in either Miller or Smith. Moreover, this purported requirement cannot be squared with the myriad of federal cases that permit the government to acquire third-party records, even when individuals do not "actively submit" the information contained in the records.

For starters, courts have attached no constitutional significance to the distinction between records of incoming versus outgoing phone calls. The technology the police used in Smith -- a pen register -- recorded only the numbers dialed by a suspect's phone. It did not (and could not) record any information about incoming calls. To capture that information, police routinely use a "trap and trace" device. If the majority were correct that the third-party doctrine applies only when an individual "actively submit[s]" information, then any effort to acquire records of incoming phone calls would constitute a search protected by the Fourth Amendment. After all, the phone customer never "actively submits" to the phone company -- "voluntarily or otherwise" -- the numbers from incoming telephone calls. Only the user on the other end of the line, who actually dials the numbers, does so.

But federal courts have not required a warrant supported by probable cause to obtain such information. Rather, they routinely permit the government to install "trap and trace" devices without demonstrating probable cause or even reasonable suspicion, the showing required for § 2703(d) orders. See, e.g., United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990). And recently we held that police "did not violate the Fourth Amendment" when obtaining a defendant's "cellular phone records," even though the records included "basic information regarding incoming and outgoing calls on that phone line." United States v.

Clenney, 631 F.3d 658, 666-67 (4th Cir. 2011) (emphasis added).[7]

Moreover, outside the context of phone records, we have held that third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection. United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). In Bynum, we explained that it "would not be objectively reasonable" for a defendant to expect privacy in his phone and Internet subscriber records, including "his name, email address, telephone number, and physical address." Id. Although we had no occasion in Bynum to consider whether an individual has a protected privacy interest in his Internet Protocol (IP) address, id. at 164 n.2, several of our sister circuits have concluded that no such interest exists. See United States v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013); United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010).

And as the majority itself recognizes, the Ninth Circuit has held that "e-mail and Internet users have no expectation of privacy in . . . the IP addresses of the websites they visit." United States v.

---

[7] Nor has this court ever suggested that other information typically contained in phone records -- the date, time, and duration of each call, for example -- merits constitutional protection. Yet a phone customer never "actively submits" this information either. Rather, this information is, to borrow a phrase from the majority opinion, "quietly and automatically calculated" by the phone company "without unusual or overt intervention that might be detected by the target user." If individuals "voluntarily convey" all of this information to their phone companies, I see no basis for drawing the line at CSLI. Notably, the majority does not provide one.

Forrester, 512 F.3d 500, 510 (9th Cir. 2008). The Forrester court also held that there is no reasonable expectation of privacy in either the to/from addresses of a user's emails or the "total amount of data transmitted to or from [a user's] account." Id. at 510-11. The court found the government's acquisition of this information "constitutionally indistinguishable from the use of a pen register that the Court approved in Smith," in part because "e-mail and Internet users, like the telephone users in Smith, rely on third-party equipment in order to engage in communication." Id. at 510.

Of course, computer users do "actively submit" some of the information discussed in the above cases, like the "to" address in an email and the subscriber information conveyed when signing up for Internet service. But users do not actively submit other pieces of information, like an IP address or the amount of data transmitted to their account. Internet service providers automatically generate that information. See Christie, 624 F.3d at 563; Forrester, 512 F.3d at 511.

If the majority is correct that the Fourth Amendment protects information individuals do not "actively submit" to third parties, then it should trouble my colleagues that we and our sister circuits have consistently failed to recognize this protection. Yet nowhere in their opinion do my colleagues even attempt to grapple with these cases or to reconcile the rule they announce with the previous applications of the third-party doctrine. Today's decision is a holding in search of a coherent legal principle; my colleagues have offered none.

C.

Instead, my colleagues rely on an argument long rejected by the Supreme Court and a series of cases involving the content of communications to support their holding that CSLI is protected by the Fourth Amendment.

First, my colleagues emphasize that cell phone use is "ubiquitous in our society today" and "essential to full cultural and economic participation." To the majority, such "ubiquitous" and "essential" use shields CSLI from the consequences of the third-party doctrine. For, the majority contends, cell phone users cannot be held to voluntarily "forfeit expectations of privacy by simply seeking active participation in society through use of their cell phones."

But the dissenting justices in Miller and Smith unsuccessfully advanced nearly identical concerns. Dissenting in Miller, Justice Brennan contended that "the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." 425 U.S. at 451 (Brennan, J., dissenting) (internal quotation marks and citation omitted). And dissenting in Smith, Justice Marshall warned that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity," i.e., a telephone, "he cannot help but accept the risk of surveillance." 442 U.S. at 750 (Marshall, J., dissenting). It was, in Justice Marshall's view, "idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." Id. The

Supreme Court has thus twice rejected the majority's "ubiquitous" and "essential" theory. Until the Court says otherwise, these holdings bind us.

Second, the majority relies on cases that afford Fourth Amendment protection to the content of communications to suggest that CSLI warrants the same protection. See Ex parte Jackson, 96 U.S. 727, 733 (1877) (content of letters and packages); Katz v. United States, 389 U.S. 347, 353 (1967) (content of telephone calls); United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (content of emails). What the majority fails to acknowledge is that for each medium of communication these cases address, there is also a case expressly withholding Fourth Amendment protection from non-content information, i.e., information involving addresses and routing. See Jackson, 96 U.S. at 733 (no warrant needed to examine the outside of letters and packages); Smith, 442 U.S. at 743-44 (no reasonable expectation of privacy in phone numbers dialed); Forrester, 512 F.3d at 510 (no reasonable expectation of privacy in the to/from addresses of emails); accord Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (noting the Fourth Amendment does not currently protect "phone numbers" disclosed to phone companies and "e-mail addresses" disclosed to Internet service providers).

The Supreme Court has thus forged a clear distinction between the contents of communications and the non-content information that enables communications providers to transmit the content.[8]

[8] In addition to being firmly grounded in the case law, the content/non-content distinction makes good doctrinal sense. The intended recipient of the content of communication is not the

CSLI, which reveals the equipment used to route calls and texts, undeniably belongs in the non-content category.

My colleagues apparently disagree with this conclusion. They posit that CSLI is "of course more than simple routing information" because "it tracks a cell phone user's location across specific points in time." But all routing information "tracks" some form of activity when aggregated over time. The postmark on letters "tracks" where a person has deposited his correspondence in the mail; a pen register "tracks" every call a person makes and allows the government to know precisely when he is at home; credit card records "track" a consumer's purchases, including the location of the stores where he made them. Of course, CSLI is not identical to any of these other forms of routing information, just as cell phones are not identical to other modes of communication. But it blinks at reality to hold that CSLI, which contains no content, somehow constitutes a communication of content for Fourth Amendment purposes.

That the majority attempts to blur this clear distinction[9] further illustrates the extent to which its

---

third party who transmits it, but the person called, written, emailed, or sent texts. The routing and addressing information, by contrast, is intended for the third parties who facilitate such transmissions.

[9] I note that my concurring colleague's concern about a general "erosion of privacy" with respect to cell phones rests on a similar misapprehension of this distinction. My friend worries about protecting the large quantity of information "stored on the phone and on remote servers." And if all that information were indeed at risk of disclosure, I would share her concern. But the Supreme Court has already made clear that police must "get a warrant" to search a cell phone for content stored on the

holding is a constitutional outlier -- untenable in the abstract and bizarre in practice. Case in point: As I understand the majority's view, the government could legally obtain, without a warrant, all data in the Sprint/Nextel records admitted into evidence here, except the CSLI. If that is so, then the line in this case between a Fourth Amendment "search" and "not a search" is the literal line that, moving left to right across the Sprint/Nextel spreadsheets, separates the seventh column from the eighth. See J.A 2656; see also J.A. 1977-79. The records to the left of that line list the source of a call, the number dialed, the date and time of the call, and the call's duration - all of which the government can acquire without triggering Fourth Amendment protection. The records to the right of that line list the cell phone towers used at the start and end of each call -- information the majority now holds is protected by the Fourth Amendment. Constitutional distinctions should be made of sturdier stuff.

III.

Technology has enabled cell phone companies, like Sprint/Nextel, to collect a vast amount of information about their customers. The quantity of

---

phone -- even for a call log listing the phone numbers a suspect has dialed. Riley v. California, 134 S. Ct. 2473, 2492, 2495 (2014). Moreover, the Riley Court suggested this rule would also apply to content stored on remote servers, i.e., the "cloud," given that "the same type of data may be stored locally on the device for one user and in the cloud for another." Id. at 2491. These are clear limiting principles. Holding, as I would, that the government may acquire, without a warrant, non-content routing information (including historical CSLI) would not send us down any slippery slope.

data at issue in this case -- seven months' worth of cell phone records, spanning nearly 30,000 calls and texts for each defendant -- unquestionably implicates weighty privacy interests.

At bottom, I suspect discomfort with the amount of information the government obtained here, rather than any distinction between CSLI and other third-party records, motivates today's decision. That would certainly explain the majority's suggestion that the government can acquire some amount of CSLI "before its inspection rises to the level of a Fourth Amendment search."[10] But this concession is in fatal tension with the majority's rationale for finding a Fourth Amendment violation here.[11] After all, the majority maintains that every piece of CSLI has the potential to "place an individual . . . at the person's home," that no piece of CSLI is voluntarily conveyed, and that the government can never know before it acquires CSLI whether the information "will detail the cell phone user's movements in private spaces." If all of this is

---

[10] It is unclear from my concurring colleague's opinion, which simply asserts that "cell site location information . . . cannot be obtained without a warrant," whether she agrees that the government can acquire a small quantity of CSLI without engaging in a Fourth Amendment "search."

[11] The lack of a bright line between permissible and impermissible amounts of CSLI also stands at odds with the Supreme Court's "general preference to provide clear guidance to law enforcement through categorical rules." Riley v. California, 134 S. Ct. 2473, 2491 (2014). I do not envy the law enforcement officers and district courts in this circuit who now must attempt to divine this line.

true (and I doubt it is),[12] then why does a cell phone user have a reasonable expectation of privacy in only large quantities of CSLI?

The majority's answer appears to rest on a misunderstanding of the analysis embraced in the two concurring opinions in Jones. There, the concurring justices recognized a line between "short-term monitoring of a person's movements on public streets," which would not infringe a reasonable expectation of privacy, and "longer term GPS monitoring," which would. Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); see also id. at 955 (Sotomayor, J., concurring). But Jones involved government surveillance of an individual, not an individual's voluntary disclosure of information to a third party. And determining when government surveillance infringes on an individual's reasonable expectation of privacy requires a very different analysis.

In considering the legality of the government surveillance at issue in Jones, Justice Alito looked to what a hypothetical law enforcement officer or third party, engaged in visual surveillance, could

---

[12] Contrary to the majority's suggestion, and unlike the information in Karo and Jones, CSLI does not enable the government to "place an individual" at home or at other private locations. Each of the cell sites at issue here covers an area with a radius of up to two miles, and each data point of CSLI corresponds to a roughly 120-degree sector of a cell site's coverage area. That translates to an area of more than four square miles in which it would be possible to "locate" a cell phone user. Although I do not think the applicability of the Fourth Amendment hinges on the precision of CSLI, it is premature to equate CSLI with the far more accurate forms of surveillance the majority cites.

reasonably have learned about the defendant. He concluded that four weeks of GPS monitoring constituted a Fourth Amendment "search" because "society's expectation" had always been "that law enforcement agents and others would not -- and indeed, in the main, simply could not -- secretly monitor and catalogue" an individual's movements in public for very long. Id. at 964 (Alito, J., concurring in the judgment) (emphasis added). In other words, when a defendant has not disclosed his location to any particular third party, the government may nonetheless surveil him, without a warrant, for as long as a hypothetical third party could reasonably "monitor and catalogue" his movements in person.

When, however, an individual has voluntarily conveyed his location to an actual third party, as Defendants did here, a court need not resort to hypotheticals to determine whether he justifiably expected that information to remain private. Here, we know that Defendants had already disclosed all the CSLI at issue to Sprint/Nextel before the government acquired the phone company's records. And the very act of disclosure negated any reasonable expectation of privacy, regardless of how frequently that disclosure occurred. The majority ignores these critical facts, applying the same constitutional requirements for location information acquired directly through GPS tracking by the government to historic CSLI that has already been disclosed to a third party.

I recognize the appeal -- if we were writing on a clean slate -- in holding that individuals always have a reasonable expectation of privacy in large quantities of location information, even if they have

shared that information with a phone company. But the third-party doctrine does not afford us that option. Intrinsic to the doctrine is an assumption that the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy. Although third parties have access to much more information now than they did when the Supreme Court decided Smith, the Court was certainly then aware of the privacy implications of the third-party doctrine. Justice Stewart warned the Smith majority that "broadcast[ing] to the world a list of the local or long distance numbers" a person has called could "reveal the most intimate details of [that] person's life." Smith, 442 U.S. at 748 (Stewart, J., dissenting). That is, in essence, the very warning that persuades the majority today. But the Supreme Court was unmoved by the argument then, and it is not our place to credit it now. If individuals lack any legitimate expectation of privacy in information they share with a third party, then sharing more non-private information with that third party cannot change the calculus.

Application of the third-party doctrine does not, however, render privacy an unavoidable casualty of technological progress. After all, Congress and state legislatures are far better positioned to respond to changes in technology than are the courts. See Jones, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."); see also In re Application (Fifth Circuit), 724 F.3d at 615 (explaining that that the proper "recourse" for those seeking increased

privacy is often "in the market or the political process").[13]

The very statute at issue here, the Stored Communications Act (SCA), demonstrates that Congress can -- and does -- make these judgments. The SCA imposes a higher burden on the government for acquiring "the contents of a wire or electronic communication" than for obtaining "a record . . . pertaining to a subscriber . . . or customer" of an electronic communication service. 18 U.S.C. §§ 2703(a), (c). And the SCA is part of a broader statute, the Electronic Communications Privacy Act of 1986 (ECPA), which was enacted in the wake of Smith. See Pub. L. No. 99-508, 100 Stat. 1848. In the ECPA, Congress responded directly to Smith's holding by requiring the government to obtain a court order before installing a pen register or "trap and trace" device. See 18 U.S.C. § 3121(a). Although Congress could undoubtedly do more, it has not been asleep at the switch.

---

[13] The majority posits that it is our responsibility to ensure that "a technological advance alone cannot constrict Fourth Amendment protection for private matters that would otherwise be hidden or inaccessible." But this is simply an incorrect statement of Fourth Amendment law. As the Supreme Court explained in Kyllo, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." 533 U.S. at 33-34. The "technology enabling human flight," for example, "has exposed to public view . . . uncovered portions of the house and its curtilage that once were private." Id. at 34. And yet the Court held in California v. Ciraolo, 476 U.S. 207, 215 (1986), and again in Florida v. Riley, 488 U.S. 445, 450 (1989), that police observations of the curtilage from an aircraft do not implicate the Fourth Amendment. See Kyllo, 533 U.S. at 34.

Ultimately, of course, the Supreme Court may decide to revisit the third-party doctrine. Justice Sotomayor has suggested that the doctrine is "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." Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring). Indeed, although the Court formulated the third-party doctrine as an articulation of the reasonable-expectation-of-privacy inquiry, it increasingly feels like an exception.[14] A per se rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy.

The landscape would be different "if our Fourth Amendment jurisprudence cease[d] to treat secrecy as a prerequisite for privacy." Id. But until the Supreme Court so holds, we are bound by the contours of the third-party doctrine as articulated by the Court. See, e.g., Agostini v. Felton, 521 U.S. 203, 237 (1997) (reversing the Second Circuit but noting that it had correctly applied then-governing law, explaining that "if a precedent of this Court has

---

[14] Seizing on the word "exception," my colleagues suggest that I advocate "an expansion" of the third-party doctrine. They misinterpret my statement as to what the third-party doctrine has become for a statement as to what the doctrine should be. This mistake is puzzling given my colleagues' reliance on Justice Sotomayor's opinion in Jones. It is clear from her opinion, though not from the majority's retelling, that tailoring the Fourth Amendment to "the digital age" would, in Justice Sotomayor's view, require the Supreme Court to "reconsider" the third-party doctrine. See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring).

direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls" (internal quotation marks, alteration, and citation omitted)). Applying the third-party doctrine, consistent with controlling precedent, I can only conclude that the Fourth Amendment did not protect Sprint/Nextel's records of Defendants' CSLI. Accordingly, I would hold that the government legally acquired those records through § 2703(d) orders.

* * *

Time may show that my colleagues have struck the proper balance between technology and privacy. But if the majority is proven right, it will only be because the Supreme Court revises its decades-old understanding of how the Fourth Amendment treats information voluntarily disclosed to third parties. Today the majority endeavors to beat the Supreme Court to the punch. Respectfully, I dissent.

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 Public Defender. ECF No. 19 ("ACLU Br."); ECF No. 20 ("EFF Br."). The government

[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.

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 govern-ment 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

---

[2] The original panel opinion, authored by D.C. Circuit Judge David Bryan Sentelle sittingby 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).

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 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

[3] A "search" also occurs for Fourth Amendment purposes "[w]hen the Government obtains information by physically

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.

---

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.

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 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,

---

[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)).

however, that "even short-term monitoring" raises concerns under *Katz* because "GPS 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_MobilePrivacyManagement.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-thanbrand-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. 735M (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 &

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

[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.

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 Florida Supreme Court, citing the Third Circuit's opinion, concluded that the third-

---

[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. 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.*

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 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

---

[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

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.

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

---

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).

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

---

[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

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).

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

---

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.

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 whole-heartedly 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 not

---

[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.*

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

---

[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

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

---

indication that any of these passive activities will generate CSLI.

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 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 emailed 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 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