PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH 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:**

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

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 Doll

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

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

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-

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.

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

(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

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

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 (1983P.E -276ub6 , S

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

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.

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 phone users' expectation of privacy in their long-term CSLI. See, e.g., Augustine, 4 N.E.3d at 865-

[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.

66 (reasonable expectation of privacy in location information

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

---

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 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

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, 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-

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 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-

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

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] Investigators and prosecutors must have

---

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 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.

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 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

[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 t48 re f intr

Appellants' 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 would frame the question as "whether an individual has a reasonable expectation

---

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.

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.

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 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

"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 th ot1 lrd Pat 2TJ 0 Tw (vealsumen to lhe)Tj 0 informatj (.)Tj (Id.)Tj ( )Tj 1f5 21271 22..2 21.6 0.48 re f EMB ET /P <<

reasonable expectation of privacy. We decline to apply the third-party doctrine in the present case because a cell phone

(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.

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

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]

[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

U

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 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

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

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 previously

[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 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.

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

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.

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

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

expectation of privacy in their long-term CSLI.[22] Specifically, we conclude that the 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

---

[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.").

[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."

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 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

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

We find no "inherent contradiction on the face of the SCA."

inapplicable where a prosecutor fails to exercise a statutory grant of discretionary power within constitutional bounds. In a related case prior to 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,

[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.

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.

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

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

[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

[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 Graham. Testimony that [redacted] 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]

[redacted] The cell phone records obtained by the government disproved this version 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

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,

establish abuse of discretion, "a defendant must show that he was prejudiced by the denial of a severance motion . . . ." Id. (citation omitted).

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 'paifacipated in the same a <uor transa <ion, or in the same series of a <s or transa <ions, 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 effaciency 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 specifac 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 sepaiate trial would offer a better chance of a quittal.'" 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

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

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). "

> 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

lik

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

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.

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 "'

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

---

[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.

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.

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 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

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 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 idenfacy 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

[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.

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

[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.);

majority is forced to rest its holding on three inapposite state cases and three district court opinions --

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 before the provider can create such a record, it must receive information indicating that a cell phone user is relying on a

---

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_PublicPerceptionsofPrivacy_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.

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

these cases make clear that the third-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

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

[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 es co-10er e 1C BT 0 Tw 12 -( )Tj ET YetAmf elec0on. Ye

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 "

the content.[8] 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.

[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 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.

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

[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

- 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 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

[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."

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 . .

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 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

and trace" device. See 18 U.S.C. § 3121(a). Although Congress could undoubtedly do more, it has not been asleep at the switch.

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