No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Sixth Circuit

AMICUS CURIAE BRIEF FOR NATIONAL DISTRICT ATTORNEYS ASSOCIATION IN SUPPORT OF RESPONDENT

Nelson O. Bunn, Jr.
Acting Executive Director
NATIONAL DISTRICT ATTORNEYS ASSOCIATION
Amicus Curiae
1400 Crystal Drive, Suite 330
Arlington, Virginia 22202
703-519-1666
nbunn@ndaajustice.org

John M. Castellano
Counsel of Record
125-01 Queens Boulevard
Kew Gardens, New York 11415
718-286-5801
jmcastellano@queensda.org

Linda Cantoni
Karen J. Friedman
Of Counsel

October 2, 2017

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitution and Statutes

Other Authorities

STATEMENT OF INTEREST[1]

The National District Attorneys Association is the largest association of prosecuting attorneys in the country, representing 2,500 elected and appointed District Attorneys across the United States, as well as 40,000 Assistant District Attorneys. NDAA provides professional guidance and support, serves as a resource and education center, and follows and addresses criminal justice issues of national importance.

As active prosecuting attorneys, NDAA and its members are uniquely knowledgeable about the important investigative uses of cell site location information in state prosecutions, including developing probable cause, verifying information provided to law enforcement, and dispelling suspicion where it is unwarranted. In addition, members regularly use grand jury subpoenas to obtain third-party business records to advance their investigations of public corruption, identity theft, stalking, economic fraud, technology crimes, and countless other offenses – investigations that would be seriously threatened if the third-party doctrine were eliminated or heavily restricted, as amici and petitioner suggest.

SUMMARY OF ARGUMENT

In the course of investigating a four-month-long string of armed robberies in Detroit, prosecutors obtained three separate court orders under section 2703(d) of the Stored Communications Act for historical cell site location information (CSLI) – records created and maintained by wireless telecommunications providers reflecting the location of the carriers' cell towers used to route phone calls made and received by petitioner. The CSLI, collected by the

---

[1]No counsel for a party authored this brief in whole or in part, and no entity or person other than amici and their counsel made a monetary contribution intended to fund the preparation or submission of this brief. Both parties have granted blanket consent to amicus filings.

carriers for their own business purposes, placed petitioner's cell phone within one-half to two miles from the specified tower and within a 60 or120 degree radial wedge at the time of a call, covering from 35 city blocks to an area 28 times that large.

The government's actions in obtaining this information did not violate the Fourth Amendment. The orders did not direct a search or seizure of petitioner himself, his home, any paper he created, maintained or possessed, or any other of his physical effects.

Nor did petitioner have any reasonable expectation of privacy in the CSLI. The records and data were created and maintained by the carriers concerning their own infrastructure for their own business purposes; the data consisted purely of routing information, not content; and he himself relinquished the information when he used the carrier's network knowing, through his carrier's privacy policy, that this information was collected and could be provided to law enforcement. *See, e.g., Smith v. Maryland*, 442 U.S. 735 (1979) (no expectation of privacy in phone numbers dialed to route calls); *United States v. Miller*, 425 U.S. 435 (1976) (no expectation of privacy in financial information in bank records).

Petitioner contends, however, that this third-party information is his property, which the government could not seize without a warrant; that the information was highly sensitive, and therefore he had a reasonable expectation of privacy in it; and that he did not relinquish his information voluntarily because cell phones are an essential part of modern life. These objections are unavailing.

First, the property-based analysis of the Fourth Amendment aims to preserve the protections in existence at the time of the Amendment's passage, *see United States v. Jones*, 565 U.S. 400, 406 (2012), and petitioner provides no support for the proposition that

the framers would have understood information necessarily disclosed as part of a business transaction with a third party as protected property.

Second, CSLI is no more sensitive than other information that this Court has held is outside the Fourth Amendment when relinquished to a third party for a business purpose. Indeed, the precise numbers dialed by a phone customer are far more revealing as to her associations and affiliations than is her presence somewhere within an area covering many dozens of city blocks.

Similarly, when this Court decided *Smith*, landlines were considered just as indispensable a part of modern life as cell phones are now, providing essential business, social, and emergency uses. Yet this Court held that consumers' business transactions with the phone company were sufficiently voluntary to relinquish any privacy interest.

Moreover, this Court should not, as petitioner implicitly suggests and some amici explicitly avow, eliminate the third-party doctrine. To do so would preclude SEC and IRS summonses for financial information necessary for their functioning and would bring a halt to countless state prosecutions dependent upon review of third-party records, including public corruption, identity theft, insurance fraud, and stalking. It would also obstruct state grand juries from issuing document subpoenas for information necessary to their functioning.

Finally, even if there were an expectation of privacy in CSLI, it would undoubtedly be a diminished one, and the use of the SCA order here would be constitutionally reasonable. The statutory requirement of "specific and articulable facts" showing materiality and the necessity of prior judicial review and approval prevent the type of abuses petitioner predicts.

CSLI RECORDS AND THEIR INVESTIGATIVE USES

CSLI identifies the location of carriers' cell towers that are used in connecting customer calls and is generated, collected, and maintained by the carrier both for engineering reasons and for business purposes related to customer accounts. As noted above, in urban areas, cell towers are usually within one-half to two miles of the phone during the call, covering between 35 average-sized city blocks and an area 28 times that size,[2] but in rural areas, signals may extend as much as 20 miles (JA 47).[3]

The tower identified in these records need not have been the closest one to the phone, as network and environmental factors affect which tower is used to complete the call (JA 82-83). Even a call from a static location may switch towers in the middle of the conversation (JA 83), and two individuals riding in the same car may use two different towers to complete their calls. The records here, and those typically provided by carriers, do not reflect the use or existence of any cell signal equipment other than standard towers, such as "femtocells," "picocells," or "microcells" with smaller coverage areas.[4]

---

[2]The area covered encompasses 3.5 million to 100 million square feet, *United States v. Carpenter*, 819 F.3d 880, 889 (6th Cir. 2016), which converts to city blocks at an average rate of 100,000 square feet per block. *How Big Is a City Block?* www.land4ever.com/block.htm (accessed 9/26/2017).

[3]Numbers preceded by JA refer to the Joint Appendix and those preceded by PB to Petitioner's Brief.

[4]These "small cells" are often purchased by customers to expand access within a building or confined area, but do not expand the towers available to the general public and are generally not reflected in CSLI. Prepared Statement of Mark Eckenwiler, Hearing on Geolocational Privacy before the Subcommittee on Crime, Terrorism, Homeland Security and

CSLI does not reflect cell towers to which the phone connected while the phone was simply powered on, or cell towers used for the purpose of conveying any other data transmitted to or from the phone, such as for "apps" on a smart phone. Similarly, CSLI does not reflect GPS or other satellite-based data, or any real-time location information. Nor did law enforcement or the carriers involved in this case cause petitioner's phone to connect with the tower or otherwise seek out his location.

Orders for CSLI obtained under section 2703(d) have many important uses at the investigative stage of serious cases, either to build probable cause to obtain warrants or to dispel suspicions of those without blame. Investigators use available geolocation evidence as a filter to winnow out and prioritize leads from the unorganized mass of related and unrelated information that surrounds a crime and a crime scene.[5]

For example, where a case presents multiple suspects with strong motives to have committed a murder and possible access to the victim, CSLI may eliminate some or all of these individuals from suspicion by establishing they were elsewhere at the time of the crime.

CSLI may also be used to verify information provided by a confidential informant, helping law enforcement determine whether the information is reliable – an important showing in establishing probable cause and one that is required in some states. Similarly, CSLI can be used to corroborate or question the accounts of other witnesses, including some who

---

Investigations, No. 111-34 at 11 (April 25, 2013).

[5]Testimony of Peter Modaferri, International Association of Chiefs of Police, Hearing on Geolocational Privacy, *supra*, n. 4, at 19-20, 23.

are purporting to cooperate, but may be withholding critical information.

CSLI may also provide important clues in cases where homicide victims are found but little is known about the events leading up to their deaths. The victim cannot consent to the disclosure of the information, but CSLI may be critical in retracing the victim's steps and locating others who may have come in contact with the victim. Similar information may be important in determining the whereabouts of other non-communicative victims, such as those in a coma, and victims and witnesses who are frightened or reluctant to provide information, including domestic violence victims.

ARGUMENT

I. Cell Phone Users Have No Cognizable Fourth Amendment Interest in Records Created and Maintained by Third-Party Carriers about the Routing of Communications through Their Networks.

For most of our history, "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *Jones*, 565 U.S. at 406. Added subsequently was the notion that government conduct obtaining access to an area or item in which the defendant had a legitimate expectation of privacy constituted a search under the Fourth Amendment, requiring that search to be reasonable. *See Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). Applying these tests here, cell phone users can show neither a trespass upon protected areas nor a legitimate expectation of privacy in the records of wireless carriers.

The records here were created and maintained by wireless carriers, and contained data generated by and about their networks, which they had built and

maintained. Obtaining this information from the carrier did not require a search or seizure of petitioner's home or person, and the records were neither a paper nor effect of petitioner. Indeed, records of the operation of a business have for at least a century been considered outside the scope of the Fourth Amendment, as they are not papers or effects of the customer. *See Miller*, 425 U.S. at 440 ("the documents subpoenaed here [defendant's bank statements and copies of checks] are not respondent's 'private papers'. . . [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks."); *Fisher v. United States*, 425 U.S. 391, 414 (1976) (accountants' workpapers and analyses not "private papers" of client); *Donaldson v. United States*, 400 U.S. 517, 522 (1971) (no Fourth Amendment issue in service of IRS summons on third party for financial records, "a question [that] appears to have been settled long ago"; citations omitted).

Similarly, wireless customers have no reasonable expectation of privacy in CSLI. First, the records contain information about the operation of the carrier, specifically the equipment and technology used to provide wireless services, and are generated for the carrier's own engineering and business purposes. A customer ordinarily has no expectation of privacy in records of how a business provides its services, such as how a power plant provides his electricity or where FedEx holds her packages. And while operational information may reflect certain facts about customer usage (the consumption of kilowatt hours at home or a penchant for sending flowers to a particular address), this information does not create a reasonable expectation of privacy in it. Indeed, the mere presence of information collected by another in the hands of a third party does not create a reasonable expectation of privacy in it, as a third party is ordinarily free to provide that information to the government and the government is free to seek it out. *United States v. White*, 401 U.S. 745, 749 (1971).

Second, to the extent that the carriers' records of the location of the cell towers a customer uses provides information about his location, he cannot claim a legitimate expectation of privacy, as he knowingly provides that information to the company in order to obtain its services.

Two seminal cases from this Court illustrate the principle. In *United States v. Miller*, 425 U.S. at 435, the government obtained by subpoena three months of defendant's bank statements and other financial records, including copies of individual deposit slips and checks. Defendant asserted an expectation of privacy in these records but this Court rejected the argument, reasoning that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." *Id.* at 442. The Court continued, "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443.

In *Smith v. Maryland*, 442 U.S. at 735, the Court held that the defendant had no "legitimate" expectation of privacy in the numbers he dialed on his home phone. The Court reasoned that phone customers "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id.* at 743. According to the Court, knowledge of the phone company's ability to keep call records was evidenced by the detailing of long-distance numbers on their statements subject to a special rate structure, and the statements in phone books that companies "can frequently help in

identifying to the authorities the origin of unwelcome and troublesome calls." *Id.* Even though customers were required to convey the information to use the phone company's services, this Court concluded that the defendant "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." *Id.* at 744.

Here, as in *Smith*, cellular customers who contract for and use services know, or reasonably should know, that their cell site location information is collected for business purposes and may be provided to law enforcement. Indeed, in making calls, customers know that they must be near a cell tower, or they cannot make a call. They must also be aware that the carrier knows the location of its own towers and that it has the capacity to collect and store that information. Indeed, if a customer wanders outside her home network, her phone tells her that she is roaming on another carrier's cell towers and subject to a special rate structure, just like the long-distance toll records in *Smith* alerted customers that the numbers they dialed were stored.

Thus, just as in *Smith*, wireless customers, by placing calls, convey the information necessary to complete the call and do so knowingly in order to obtain services. Indeed, here, petitioner had all the more reason to understand the risk he was assuming: carrier privacy policies explicitly state that this information will be provided to law enforcement upon the service of a subpoena or other legal process.[6] Just

[6]Verizon, for example, specifically informs customers that it collects "wireless location" information and automatically monitors their connections, in part to "prevent our networks, services and users from fraudulent, abusive, or unlawful uses." Full Privacy Policy, Verizon, 2017. Verizon also advises customers that it "may

as phone customers could be expected to know information in their phone books in *Smith*, modern cell phone users should be expected to know information about their carriers' privacy policies. Indeed, wireless customers are required to acknowledge those policies at the time they enter into a contract as part of the terms of service, providing all the more reason they should know their contents.

Third, customers have no reasonable expectation of privacy in CSLI because it consists of only routing information, rather than the content of any communication. In the communications context, this Court has long drawn the distinction between information that is required in order to convey a communication and its content. Beginning with *Ex parte Jackson*, 96 U.S. 727, 733 (1878), this Court held that information required to deliver a communication, such as a physical address, is not constitutionally protected, even though it might bring embarrassment. "In a small village, for instance, a young gentleman may not altogether desire that all the loungers around the store which contains the Post-office shall be joking about the fair object of his affections." *Our Letters*, N.Y. Times, Dec. 12, 1872, at 4. Similarly, in *Katz* and *Smith*, this Court distinguished between the content of a call, which was protected, and the information necessary to complete it, which was not.

The location of the cell towers used to complete petitioner's calls unquestionably falls on the non-content side of that line. It is literally routing information – the route taken by the radio signals to complete petitioner's call. Nothing about the content

---

be required by law to disclose personally identifiable information to a governmental entity to comply with valid legal process, such as warrants, court orders or subpoenas." *Id.* In addition, Verizon's transparency reports specifically inform customers that location information is provided to law enforcement, including the precise number of requests. *See* Verizon Transparency Report, First Half, 2017.

of any call or message was disclosed, and the information was necessary to complete the call. It is, as this Court put it in *Smith*, "a means of establishing communication," not the communication itself. 442 U.S. at 741.

II. Petitioner's Arguments Fail to Establish that He Had a Property Interest or a Reasonable Expectation of Privacy in His Carrier's Records Sufficient to Invoke the Fourth Amendment.

A. Petitioner Has No Cognizable Property Interest in His Carrier's Records.

Petitioner argues that he has a property interest in the records because federal law generally limits its disclosure to others. This argument is flawed for several reasons. First, similar protections exist for bank records and for the numbers dialed on a telephone, yet petitioner does not dispute that these records remain outside the Fourth Amendment (PB 35).

Second, while Congress did enact protections for this information, it also expressly limited them by permitting disclosure of cell-site records in a variety of circumstances without a customer's consent, 47 U.S.C. 222(c)(1) and (d)(1)-(4), and by granting access to this very same information to the government upon a proper showing under the SCA. Petitioner cannot cite Congress's limited protections as creating a right and then transmogrify that limited right into an absolute right by assuming Fourth Amendment protection.

Third, the property-based Fourth Amendment analysis seeks to preserve the amount of privacy that existed at the time of the Amendment's passage, *see Jones*, 565 U.S. at 406, and it is highly doubtful that the founders would have believed that information they provided to others as part of a business transaction constituted their personal property.

Indeed, if a founder-era employee or independent contractor provided a detailed list of his travel and expenditures over a period of weeks or months to another for the purpose of obtaining reimbursement, it is unlikely he would believe this information constituted his property. Nor is there any evidence that a founding-era citizen would believe that information or records about the internal functioning of a business with whom he has contracted was somehow his property, or otherwise his "papers or effects."[7]

Indeed, if anything, the law at the time appears to have allowed third-party business records, which routinely convey information about transactions with customers, to be obtainable by subpoena, and therefore outside the Fourth Amendment's warrant requirement. *Wilson v. United States*, 221 U.S. 361, 373 (1911) (compelling compliance with subpoena *duces tecum* for corporate records and tracing its history to before the reign of Charles the Second).

B. The "Sensitive" Nature of the Information Held by Third Parties Does Not Alone Create a Reasonable Expectation of Privacy.

Petitioner and amici argue that customers have a reasonable expectation of privacy in CSLI because the information at issue is particularly sensitive and personal, and may reveal associational activities within the sphere of the First Amendment (PB 36-38). But even sensitive information conveyed to, or in the hands of, a third party, does not by itself give rise to a cognizable Fourth Amendment interest.

---

[7] In 1791, "effects" were defined merely as "goods" or "moveables." T. Sheridan, Dictionary of the English Language (1780); S. Johnson, Dictionary of the English Language (1802); J. Kersey, A New English Dictionary (1702) ("the Goods of a Merchant").

Indeed, even the most personal information trusted to a confidant could be disclosed to law enforcement when in the hands of a third party, including highly incriminating admissions. *United States v. White*, 401 U.S. at 749 ("however strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent . . .").

The same applies to information provided to third parties in business transactions. Bank records contain what is generally considered to be highly private information, one's personal finances, which could reveal not only one's associations, but also precise dollar amounts conveyed to them, as well as the account holder's personal investments, donations to religious or charitable institutions, and the amount and purpose of loans and other credit. And the records obtained in *Miller* extended through three months of bank statements, potentially providing a telling picture of the defendant's associations, habits, and even opinions. Similar financial records could be even more revealing, such as credit card records, which provide a detailed list of where and when purchases are made.

Perhaps even more revealing are the phone numbers dialed from one's home. A record of phone calls made and received provide a detailed list of virtually all of one's associations – one far more precise than the wide-swath locational data conveyed by CSLI.

Yet, this Court specifically rejected arguments in *Miller* and *Smith* concerning the sensitive or confidential nature of the information at issue. In *Miller*, the Court upheld the disclosure of banking information over the dissent's objection that "in the course of his dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography." 425 U.S. at 451 (Brennan, J., dissenting). The *Miller* Court also

rejected the conclusions of *Burrows v. Superior Court*, 13 Cal.3d 238 (1974), quoted by the dissent, that depositors consider their information private and confidential, as two bank representatives had specifically testified in that case.

Petitioner, however, distinguishes the locational information at issue here, claiming it is far more private or confidential. He claims, in part, that locational data reaches into the home, an area specifically protected by the Fourth Amendment (PB 17-18). But this Court rejected the same contention in *Smith*, where the defendant argued that he demonstrated an expectation of privacy by his conduct because he used the telephone from his own house. As this Court explained, "the site of the call is immaterial for purposes of analysis in this case. . . . Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call." 442 U.S. at 743. Thus, even assuming that the far less specific cell tower data here would be sufficient to place petitioner in his home, he necessarily conveyed that information in order to complete his call.

Petitioner nevertheless points to *United States v. Jones*, 565 U.S. at 406, as evidence that customers have an expectation of privacy in their location information, at least as aggregated over time. There are at least three critical differences, however, between *Jones* and this case. In *Jones*, the concurring justices expressed concern over satellite-based GPS location data, capable of pinpointing an individual's location to within 50 feet, because it "enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." 565 U.S. at 416.

By comparison, CSLI is far less revealing, quantitatively and qualitatively. Indeed, within the area covered by cell towers – between 35 city blocks and an expanse 28 times that large – an individual

could be at one of hundreds, if not thousands, of residences or businesses, precluding the reader from distinguishing between "a visit to a gynecologist, a psychiatrist, a bookie, or a priest," as petitioner contends (PB 17). And the more rural the locations, the greater the cell tower coverage, up to 20 miles. This lack of specificity is critical because CSLI does not provide the kind of associational information found troublesome by the concurrers, much less the ongoing detailed biography over time that so concerned them. *See Smith*, 442 U.S. at 742 (citing pen register's "limited capabilities" in determining that records of specific numbers dialed by defendant was not covered by Fourth Amendment). Indeed, CSLI, because of its lack of specificity, is never conclusive evidence on its own – it always has to be combined with other evidence to be meaningful, as it was in this case.

Nor does the assertion that other types of cell tower data could provide more specific information change the analysis (PB 27-28). No "microcells," "femtocells," or other small-range tower information was contained in the carriers' records here, and it ordinarily is not. Similarly, distances from the tower are not ordinarily calculated or reflected in CSLI. As this Court has noted, in interpreting the Fourth Amendment, it is important to specify the precise nature of the records obtained, rather than speculating about other technologies and their potential uses. *See Smith*, 442 U.S. at 741.

Second, unlike in *Jones*, here petitioner himself conveyed the location information to another as part of a business transaction to obtain specified services under circumstances where he either knew or should have known that this type of information was collected, and could be provided to law enforcement. While in *Jones*, the police surreptitiously planted a GPS device providing information directly to them, here petitioner knowingly provided the information to a third party as part of a business transaction in order to obtain a benefit. This Court's decisions in *Smith*, *Miller*, and

other cases preclude the finding that such information is private or protected under the Fourth Amendment.

C. Petitioner Has Not Shown That He Acted Involuntarily in Providing CSLI.

Petitioner and amici, however, argue that this case is distinguishable from *Miller* and *Smith* because customers do not "voluntarily" provide CSLI to their carriers. They argue that cell phone use is effectively compelled in modern society and that customers thus have no choice but to convey cell site location information (BP 35).

But in the pre-digital era, use of landline phones was considered just as essential, yet this Court held that the numbers dialed were not within the Fourth Amendment. Indeed, before cell phones, landline phones, in common use for many decades, were used for every facet of daily life, including social interaction, business transactions, and emergency services. Nor were there other readily-transmitted means of communication that are available now, like emails, making phones all the more essential then. The fact that phone service was an indispensable feature of virtually every home and that phone numbers had to be conveyed to obtain that service did not render the relinquishing of this information any less voluntary, in this Court's view.

Similarly, at the time *Miller* was decided, use of banking and personal credit services were an essential facet of everyday life, yet the information conveyed in order to obtain those services does not enjoy Fourth Amendment protection. And this Court so held in *Miller* despite the specific objection that, "[f]or all practical purposes, 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.

Nor is it true, as petitioner contends, that he was unable to restrict the conveyance of his CSLI, even when at a sensitive location. Indeed, while the defendant's calls from his home in *Smith* necessarily required him to convey the numbers dialed, today's smart phone options allow users to minimize the provision of CSLI with little effort. Petitioner could have, for example, used any number of common smart phone applications to complete calls or otherwise confer with his friends or associates without providing CSLI.[8] And, of course, petitioner could have placed his phone on "airplane" mode, turned it off, or simply left it at home, in his car, or at any secure location. But he did none of these, suggesting his concern for locational privacy was simply not that great.

D. Petitioner's Argument That He Reasonably Expected that His Information Would Not Be Disclosed to Law Enforcement Is Unavailing.

Petitioner argues that even if he knew that the location of the cell towers used to complete his calls would be conveyed to the carrier, he still had a reasonable expectation that it would not be turned over to law enforcement. This argument is both counter-factual and foreclosed by *Smith* and *Miller*.

First, both *Smith* and *Miller* held that even though the defendants released their information to

---

[8]Universally available free applications like "WhatsApp?" and "Viber" provide the ability to text message and make and receive phone calls through internet connections that are not reflected in CSLI. *See, e.g.*, *WhatsApp, Making Voice Calls,* 2017, https://faq.whatsapp.com/en/android/28000016. Applications like "Skype" and "Facetime" use similar technology to permit audio and video calls and are not reflected in CSLI. Users of these applications number in the billions. *See, e.g.*, Statista, *Number of Monthly Active WhatsApp Users*, https://www.statista.com /statistics/260819/number-of- monthly-active-whatsapp-users (1.3 billion).

specific third parties, and might have expected confidentiality as to the government, the information was afforded no constitutional protection. *See Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 443.

Second, even if that argument were not foreclosed, cell phone users either know or should know of the specific risk that CSLI could be provided to law enforcement. Carriers' privacy policies, which customers are required to accept as a condition of receiving service, disclose that CSLI can be, and is, turned over to law enforcement upon proper legal process.

E. Petitioner's Attempt to Raise the Specter of Unrestrained Privacy Violations Is Unfounded.

Petitioner nevertheless warns that if the third-party doctrine is "extended" to CSLI, it will allow the government unrestrained access to every type of digital information, whether accessed on a cell phone or otherwise. He argues that police will have license to track every American at will, that his emails will be hacked by law enforcement, and that his most intimate opinions and thoughts will be collected by the government. Indeed, he speculates that there is already evidence of law enforcement's rampant abuse of CSLI.

This is simply not so. First, an affirmance here would not by itself permit "tracking" of citizens. Indeed, no real-time locational information is at issue, nor did prosecutors cause the company to send a signal or "ping" petitioner's phone to discern its location. *United States v. Graham*, 824 F.3d 421, 425-26 (4th Cir. 2016) (explaining that "[n]o government tracking is at issue here"). Moreover, the general historical information that was requested requires a court order under the SCA and thus cannot be acquired wholesale or mined by law enforcement.

Similarly, petitioner's and amici's allegations of abuse of CSLI are without foundation. While citing statistics from carriers' transparency reports on the numbers of requests made for such information, they make no effort to put those absolute numbers in context. For example, they do not compare the number of requests to the number of subscribers of the same company, much less the number of days of CSLI requested to the number of days subscribers used their phones. Moreover, even the roughest comparison belies petitioner's position. For example, Verizon's 53,532 requests, cited by the Electronic Frontier Foundation in their brief (p. 13-14), as compared to its more than 142 million subscribers[9] reveals that law enforcement obtains only the tiniest shard of this type of information – less than one-hundredth of a percentage point – hardly the dragnet so frequently alleged.[10] And the EFF makes no effort to compare the information to the number of subpoenas issued for bank records, numbers dialed, or other records obtainable by subpoena.

Moreover, lower courts applying the third-party doctrine have still thoughtfully afforded constitutional protections to a great variety of private data. Courts, for example, have adhered to the traditional distinction between content and conveyance of messages, ensuring that the contents of any email or text message will fall within the Fourth Amendment. *See, e.g., United States*

---

[9]Fierce Wireless, *How Verizon, AT&T, T-Mobile, Sprint and More Stacked Up in Q2 2016* (Aug. 15, 2016).

[10]Other evidence points to a restrained use. For example, in Queens, New York, the 10th most populous county in the nation with 2.3 million inhabitants and more than 54,000 prosecutions in 2016, prosecutors obtained CSLI orders only 92 times. Castellano, *Justices Poised to Consider, or Reconsider, Fourth Amendment Doctrines*, SCOTUSBlog http://www.scotusblog.com/2017/08/symposium-justices-poised-consider-reconsider-fourth-amendment-doctrines-assess-scope-privacy-digital-age (Aug. 1, 2017). More than half of these orders were for ten days or less, and only seven exceeded 90 days, mostly for pattern crimes. *Id.*

v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). Social network pages are also ordinarily simply messages to a limited group of friends and thus protected substantive communications. And similar content-based distinctions could be made with regard to other types of digital information, including, for example, one's internet searches or other expressive information. In addition, images and documents stored digitally by third parties are readily analogized to other types of storage containers, like lockers, that are provided by third-party bailees and require a warrant to open.

True, a limited amount of information conveyed to third parties reflecting business transactions might be accessible to the government, upon a proper showing under the SCA. But this same business information would have been accessible before the advent of the digital age, including in the most robust economy when such transactions were abundant. In many, if not most, cases, it makes little difference whether information formally written in ledgers is now held digitally: the taxi dispatcher's written records of a customer's trip, including the timing and destination, are not so profoundly different from Uber's records of its customers' trips that the two situations demand different constitutional treatment.

And, to the extent that these business transactions have increased or that different types of information may be conveyed by the customer, most Americans understand that there is a necessary diminution of privacy in the digital era, and are willing to accept the tradeoff. *See Jones*, 565 U.S. at 427 (Alito, J., concurring) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable").

This is not to say that individuals do not *desire* privacy, even as they release their information to others. But there is a distinction between desiring privacy and reasonably expecting it. As Judge Wilkinson wrote concurring in *United States v. Graham*, 824 F.3d at 441: "It is human nature, I recognize, to want it all. But a world of total privacy and perfect security no longer exists, if indeed it ever did."

Petitioner relies on *Riley v. California*, 134 S.Ct. 2473 (2014), to argue that doctrines from the pre-digital era cannot be woodenly applied to digital data. Neither can they be entirely ignored. Indeed, in *Riley*, this Court expressly referred to other exceptions to the warrant requirement that could apply to cell phones, or to some portion of the information in them. *Id.* at 2494. Here, CSLI falls squarely within the third-party doctrine and the well-established distinction between content and non-content applicable to communications. Moreover, the ability to access CSLI is far less intrusive than the virtually unlimited permission of law enforcement sought in *Riley* to scavenge through the wealth of information available on a modern smart phone. *Riley*, then, does not advance petitioner's argument.

F. Petitioner's Position Would Require Overturning the Third-Party Doctrine, Thereby Dangerously Altering the Balance of Public and Private Interest in the Fourth Amendment.

While petitioner attempts to distinguish *Miller* and *Smith*, these efforts fall short. *Miller* and *Smith* directly refute his arguments concerning the sensitivity of the information conveyed, the expectation that the information will not be provided to the government, and the idea that the data is entitled to protection as private papers or property. Nor can these cases be limited to their facts, as petitioner and some amici suggest.

Financial records are today created and maintained digitally and thus *Miller* would have no effect at all if limited to paper records. Nor can digital banking records be meaningfully distinguished from other information disclosed digitally in the course of business transactions. Similarly, the numbers dialed by phone users are collected digitally, and were contained on the very same document that petitioner's carriers provided here. It would indeed be anomalous if law enforcement could freely view the column of specific phone numbers contained in the carriers' records, but were precluded from seeing the location of the cell towers used to route the calls.

In short, in order to rule in favor of petitioner, this Court would have to abolish the third-party doctrine, a goal more candidly avowed by some amici than by petitioner. This conclusion belies petitioner's argument that all he seeks is the same degree of privacy he had before the advent of the digital age (PB 18); indeed, he is asking for far more, including unwarranted privacy in banking records, numbers dialed, his accountant's papers, and the myriad other forms of information conveyed to third-party businesses that previously would have been available by a subpoena *duces tecum*. The Court should reject petitioner's attempt to overturn this doctrine.

First, to do so would not only require overruling *Miller* and *Smith,* but also overturning cases extending back far earlier. This includes, for example, this Court's cases upholding document subpoenas directed to accountants and other businesses even though those subpoenas clearly disclosed information about clients. *See, e.g., Couch v. United States*, 409 U.S. 322, 336 n. 19 (1973) (accountant's client does not have "the necessary expectation of privacy to launch a valid Fourth Amendment claim" concerning seizure of accountant's records); *Donaldson v. United States*, 400 U.S. 517, 522 (1971) (upholding IRS summons to employer and employer's accountant and finding no constitutional issue; the question "appears to have been settled long

ago when the Court upheld, against Fourth Amendment challenge, an internal revenue summons issued under the Revenue Act of 1921 and directed to a third-party bank"); *Oklahoma Press Pub. Co. v. Walling*, 327 U.S. 186, 208 (1946) ("the Fourth [Amendment], if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described . . .'"). *See also California Bankers Ass'n v. Shultz*, 416 U.S. 21, 53 (1974) (rejecting Fourth Amendment challenge to Bank Secrecy Act requirements; "(I)t is difficult to see how the summoning of a third party, and the records of a third party, can violate the rights of the taxpayer, even if a criminal prosecution is contemplated or in progress").

Second, eliminating the ability of prosecutors to obtain these types of documents would stymie many types of investigations currently dependent on business documents and thereby dangerously upset the existing balance between public and private interests under the Fourth Amendment. *Camara v. Mun. Court*, 387 U.S. 523, 534 (1967) (expressing that "accommodation between public need and individual rights is essential" in interpreting the Fourth Amendment). For example, subpoenas directed to accountants, routinely used in state and federal tax prosecutions, would be precluded because the information in the hands of the accountant would consist of personal financial records subject to the warrant requirement. Similarly, subpoenas issued to financial institutions in securities fraud investigations would no longer be valid, as probable cause and a warrant would be required.

The investigation of many other crimes routinely prosecuted by state district attorneys would also come to a halt because they are dependent on subpoenas of financial records or similar third-party documents. These subpoenas allow investigators to trace funds, confirm identities, and investigate myriad types of fraud and related crimes. Investigations dependent on these subpoenas include cases involving insurance fraud, identity theft, credit card fraud, mortgage fraud,

money laundering, embezzlement, elder fraud, and the defrauding of government benefit programs.

The effect of eliminating this investigative tool in such prosecutions is staggering. Insurance fraud causes 40 billion dollars worth of losses each year,[11] and identity theft has been estimated to strike a new victim every two seconds.[12] Embezzlement prosecutions, which create *average* losses for business and government agencies of well over one million dollars per year, and disproportionately affect smaller businesses, would also be seriously impeded.[13] Nor are the investigations affected solely those for economic crimes. Public corruption prosecutions focus on financial records to trace funds, stalking cases are often dependent on records of communications, and third-party records are used in countless other prosecutions for such ordinary matters as, for example, learning who rented a car observed at the scene of a crime.

Moreover, as society generally has become computerized, criminals actively use, and hide their crimes in, the digital maze. They use Bitcoins to conduct illicit business, hide proceeds, and launder money,[14] take advantage of the increased access presented by online forums to perpetrate their frauds against the young, the gullible, and the elderly, and use internet advertising to sell child sexual services and

---

[11]FBI, Insurance Fraud Statistics, https://www.fbi.gov/stats-services/publications/insurance-fraud (accessed 9/22/17).

[12]Ellis, *Identity Fraud Hits New Victim Every Two Seconds*, CNN Money (Feb. 6, 2014).

[13]2017 *Hiscox Embezzlement Study* (Aug. 17, 2017) (available at http://www.hiscox.com/2017-hiscox-embezzlement-study.pdf) (accessed 9/20/17).

[14]Boylan, *Military, Intelligence Agencies Alarmed by Surge in Bitcoin Value in 'Dark Web' Fight*, Washington Times (Aug. 10, 2017).

illicit wares.[15] They also use technology to commit crimes in other ways not previously possible, including ransomware and tech support fraud.[16] This explosion in internet crime would become immeasurably more difficult to combat with the elimination of the third-party doctrine, impeding law enforcement efforts to simply keep pace to investigate the same crimes it would previously prosecute. "Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." *In re Historical Cell Site Data*, 724 F.3d 600, 614 (5th Cir. 2013).

Third, the abandonment of the third-party doctrine would also substantially limit the traditional power of state grand juries, which routinely issue document subpoenas in the course of their proceedings. Grand juries are an integral part of many state justice systems, and, particularly in economic crime and public corruption cases, conduct meaningful, long-term investigations into fraud and misconduct. Moreover, this Court has recognized that body's essential role and enforced its subpoenas even against First Amendment challenges. *Branzberg v. Hayes*, 408 U.S. 665 (1972). Nor was the Fourth Amendment previously seen to be incompatible with a properly issued grand jury subpoena *duces tecum* directed at a business, even though it might reflect on individual customers or officers. *Hale v. Henkel*, 201 U.S. 43, 73 (1906) ("We think it quite clear that the search and seizure clause of the Fourth Amendment was not intended to interfere with the power of courts to compel, through a subpoena

---

[15]Staff Report, US Senate Permanent Subcommittee on Investigations, *Backpage.com's Knowing Facilitation of Online Sex Trafficking* (Jan. 9, 2017) (available at https://www.hsgac.senate.gov/subcommittees/investigations/reports) (accessed 9/24/17).

[16]FBI, 2016 Internet Crime Report, at 10-11, https://pdf.ic3.gov/2016_IC3Report.pdf (accessed 9/26/17).

duces tecum, the production . . . of documentary evidence").

Fourth, the frequent criticism that the third-party doctrine misunderstands the voluntariness of the information provided to the third party should be rejected. Indeed, in some respects, information in the hands of third parties should be available to law enforcement regardless of whether it was disclosed voluntarily. If, for example, a wife hires a private investigator to follow her spouse and take notes of his comings and goings, the husband would have no standing to challenge the government's seizure of the notes, even though it contained his personal location information and even though he did not provide that information voluntarily. Similarly, an individual's location captured on a third party's private security camera, or even network of cameras,[17] may be conveyed "involuntarily" but a defendant would ordinarily have no standing to preclude a third party from releasing it.

Furthermore, the third-party doctrine's conception of voluntariness reflects a fundamental logic: "In any normal life, even in pursuing his most private purposes, the individual must occasionally transact business with other people. When he does so, he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair." *Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1043 (D.C. Cir. 1978).

Fifth, the alternative theory – that information retains its private character even as it is released to

---

[17]Large apartment complexes, private universities, and sprawling corporate campuses often have networks of surveillance cameras, and, even in their absence, police frequently contact multiple third parties with surveillance capabilities to piece together an individual's movements over time. *See, e.g., Judge Sheila Abdus-Salaam Captured Nine Times on Video Before Suspicious Death,* NY Daily News (April 28, 2017).

others or enters the stream of commerce – is fatally flawed as a constitutional doctrine. Initially, it would be impractical at best. For example, documents subpoenaed in the course of investigations of businesses could not be examined until the source of the information in the records was determined. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 581-82 (2009). Even then, law enforcement would presumably need probable cause to believe the individuals whose information is contained in the record committed a crime, a requirement this Court has rejected. *United States v. R. Enterprises, Inc.*, 498 U.S. 292, 297 (1991). The doctrine would also create other vexing questions, such as when otherwise personal information would lose its protection by being divulged to others on repeated occasions.

The alternative theory would also create other untenable results. For example, law enforcement would presumably be free to approach third parties for their oral recollections or knowledge of personal information about a defendant, including her business transactions, and grand juries could compel the attendance and testimony of such a witness, but could not obtain a written, and more precise, memorialization of that same transaction.

Moreover, as four concurring justices of this Court observed in *Jones*, "'[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." 565 U.S. at 429–30. *See City of Ontario v. Quon*, 560 U.S. 746, 759 (2010). Indeed, much of the purported social science data cited by amici would be far better presented and evaluated in legislative hearings, as would the countervailing needs of law enforcement to address criminal exploitation of

the internet.[18] There, statutory schemes can be debated, the impact of those proposals assessed by such impartial arbiters as the Congressional Budget Office, and representatives can fashion a nuanced remedy. The judicial response, by contrast, is confined to voting up or down on the specific, limited set of facts presented in particular litigation, often years or decades after the technological advances are in place. It also frequently results in circuit conflicts that ultimately require this Court to continually "update and redefine the Fourth Amendment as technology evolves" – a procedure ill-suited to technological advances that develop at breakneck speed. *See* Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 805 (2004).

Nor has Congress been inadequate to the task of creating statutory schemes to protect informational privacy, as it promptly did to regulate the privacy of banking records after *Miller*,[19] and as it has already done with regard to telecommunications and internet providers in the SCA. The statutes enacted include the precise mechanism used here, the section 2703(d) order, which balances privacy concerns and legitimate government needs by requiring pre-compliance judicial review and approval. Lower courts, including the Sixth Circuit here, have reasonably adopted that mechanism as a meaningful accommodation of interests. And, as

---

[18]The House, for example, has conducted hearings on geolocational privacy and how to address it, *see* Hearing before the House Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, No. 113-34 (April 2013), and the Senate has conducted an extensive investigation into the illicit operations of backpage.com and how to address them. *See* note 15, *supra*.

[19]*See* The Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, §§ 1100-22, 92 Stat. 3697-710 (1978).

detailed below, this conclusion presents a separate ground for affirmance here.[20]

III. Even Assuming There Were a Cognizable Fourth Amendment Interest in CSLI, Court Orders Under Section 2703(d) Would Satisfy the Fourth Amendment.

Even if this Court were to find that the petitioner had some expectation of privacy in CSLI, that expectation would necessarily be diminished for many of the reasons cited above. The 2703(d) order used here and by most prosecutors nationwide was adequate to address the concerns raised by that diminished expectation and render the government's conduct reasonable under the Fourth Amendment. Indeed, this Court may, as it has in the past, decide this case by assuming, without deciding, the existence of a cognizable interest, and finding the government conducted itself reasonably. *See NASA v. Nelson*, 562 U.S. 134, 147 (2011); *Quon*, 560 U.S. at 760. This could well be the easiest path here, and is far narrower and more certain in its scope than any ruling abolishing the well-established third-party doctrine.

Where government conduct intrudes on only a diminished expectation of privacy, this Court has on many occasions relaxed the warrant requirement, relying on the Fourth Amendment's more general command that citizens be free of "unreasonable" searches. These exceptions apply to, among other things, a person's diminished expectation of privacy in his automobile, *California v. Carney*, 471 U.S. 386, 391 (1985); the diminished expectation of privacy attendant

---

[20]In addition to finding that petitioner had no expectation of privacy in CSLI, the Sixth Circuit addressed the reasonableness of any cognizable intrusion under the Fourth Amendment, expressly rejecting the argument that the balance adopted by Congress in section 2703(d) was constitutionally inadequate. 819 F.3d at 889-90.

to a short detention rather than an arrest, *Terry v. Ohio*, 392 U.S. 1 (1968); and the diminished expectation of a probationer in his home and belongings, *United States v. Knights*, 534 U.S. 112 (2001).

In addition, this Court has held that the diminished expectation of privacy possessed by a business or corporation in its own books requires merely a subpoena, and this applies even where the records reflect information about clients or customers. *See, e.g., Couch v. United States*, 409 U.S. at 336 n. 19.

Here, even assuming a phone customer has some expectation of privacy in CSLI, that privacy interest would necessarily be diminished. This is for many reasons, including that location information is generally exposed to the public; CSLI discloses only the most general geographic areas and does not reveal specific locations or associations; CSLI consists of non-content routing information created and kept by a third party for its own business purposes; and customers relinquish the information after being informed that it is collected and may be disclosed to law enforcement.

The 2703(d) order reasonably addresses the concerns raised by these diminished expectations. The statutory provision requires a specification of the documents, a particularized showing of their relevance and materiality, and judicial intervention before the records are disclosed. Under 2703(d), law enforcement must demonstrate "specific and articulable facts" showing "reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." This required demonstration of materiality "guards against abuse . . . by way of too much indefiniteness or breadth." *Walling*, 327 U.S. at 208.

Even more importantly, the statute requires judicial intervention before compliance. This provides a critical element of the Fourth Amendment's protection because it "interpose[s] a magistrate between the

citizen and the police ... so that an objective mind might weigh the need to invade [the searchee's] privacy in order to enforce the law." *McDonald v. United States*, 335 U.S. 451, 455 (1948).

This mechanism also avoids the precise ill identified by petitioner and amici, the purported "dragnet" collection and storage of location information to be searched for any purpose whatsoever. It allows the court to review the required "specific and articulable facts," and ensure that the CSLI is relevant and material to specific crimes. And it allows the court to control not only access to CSLI in the first place but also to limit the quantity or duration of the information obtained since relevance and materiality will depend on the timing of the crimes being investigated.

CONCLUSION

Cell phone customers have no cognizable interest in carrier records identifying the towers used to route their calls, and the privacy of CSLI is nevertheless protected from government abuse by judicial intervention. The order of the Sixth Circuit should therefore be affirmed.

Respectfully submitted,

Nelson O. Bunn, Jr.
Acting Executive Director
NATIONAL DISTRICT ATTORNEYS ASSOCIATION
1400 Crystal Drive, Suite 330
Arlington, VA 22202
(703) 519-1666
nbunn@ndaajustice.org

John M. Castellano
Counsel of Record
125-01 Queens Boulevard
Kew Gardens, NY 11415
(718) 286-5801
jmcastellano@queensda.org

Linda Cantoni
Karen J. Friedman
Of Counsel

October 2, 2017