No. 12-4659

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,
***Plaintiff/Appellee*,**

v.

AARON GRAHAM and ERIC JORDAN,
***Defendants/Appellants*.**

On Appeal from the United States District Court
for the District of Maryland, Northern Division
(The Hon. Richard D. Bennett)

DEFENDANTS'/APPELLANTS' OPPOSITION TO THE GOVERNMENT'S PETITION FOR REHEARING EN BANC

JAMES WYDA
Federal Public Defender
District of Maryland

MEGHAN S. SKELTON
Appellate Attorney
6411 Ivy Lane, Suite 710
Greenbelt, MD 20770
(301) 344-0600

Counsel for Aaron Graham

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Rules

Introduction

The panel correctly decided that tracking a person using historical cell site location information (CSLI) for 221 days, without a warrant or probable cause, is dragnet surveillance that the Fourth Amendment prohibits. *See United States v. Jones*, 132 S. Ct. 945, 952 n.6 (2012). The government is essentially asking this Court to treat cell phones as personal homing beacons, providing it the wherewithal to follow and recreate a person's every movement. The government seeks to do so without a warrant or probable cause, using the excuse that telecommunications providers also happen to know when and where an individual has gone and is going.

The difference between what the government did here and what George Orwell envisioned is that Big Brother's constant surveillance through telescreens was stationary. But the surveillance here moves with citizens using a common household device carried in the pockets or purses of almost every American adult. Our Founders crafted the Fourth Amendment to require a warrant based on probable cause before the government could acquire such intimate information about a person. The panel's conclusion that the government must comply with the warrant requirement before obtaining historical CSLI correctly applies the Fourth Amendment.

Moreover, rehearing this case could not resolve the circuit splits and splits among the sovereigns, all of which existed before the panel decided this case. Whether this Court finds a Fourth Amendment violation or not, the splits will remain.

Reasons for Denying the Petition

I. Rehearing would neither clarify nor resolve the fractured state of the law regarding warrantless tracking using historical CSLI.

The government asks for rehearing en banc to resolve a split with opinions from the Third, Fifth, and Eleventh Circuits.[1] (Petition at 10-11, 14.) Rehearing, however, could not achieve this goal because the splits would remain, whether the en banc court decides that a Fourth Amendment violation occurred or not.

To begin, the government incorrectly claims that the majority's decision conflicts with a decision of the Third Circuit. (Petition at 14.) In fact, the majority states, "We conclude, in *agreement* with the analysis of the Third Circuit in *In re Application (Third Circuit)* and that of several state supreme courts, that the third-party doctrine of *Smith* and *Miller* does not apply to CSLI generated by cell phone service providers."[2] (Slip Op. at 45 (emphasis added).) The government's claim that the panel opinion conflicts with the Third Circuit is misleading at best.

---

[1] The government refers to *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (*In re Application (Fifth Circuit)*); and *In re Application of U.S. for an Order Directing Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010) (*In re Application (Third Circuit)*).

[2] *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), establish in broad terms that individuals have no reasonable expectation of privacy in information that they have voluntarily disclosed to third parties.

While it is true that the majority opinion conflicts with decisions from the Fifth and Eleventh Circuits regarding the applicability of *Smith* and *Miller* and the third party doctrine, these courts had already split with the Third Circuit. The Eleventh and Fifth Circuits held that individuals have no reasonable expectation of privacy in historical CSLI because, under *Smith* and *Miller*, individuals voluntarily disclose their location data to cellular service providers. *Davis*, 785 F.3d at 511-12; *In re Application (Fifth Circuit)*, 724 F.3d at 612-13. Several years earlier, however, the Third Circuit concluded that *Smith* and *Miller* do not apply to CSLI because individuals *do not* voluntarily convey their location data in any meaningful sense. *In re Application (Third Circuit)*, 620 F.3d at 317-18. *See also Tracey v. State*, 152 So. 3d 504, 525-26 (Fla. 2014) (holding that CSLI does not fall within the third party doctrine's exception to a reasonable privacy interest). Indeed, the split existed before, and continued after, the Eleventh Circuit addressed the issue en banc.

The Circuits, as well as several state supreme courts, are also already split on a different, but related issue: whether individuals enjoy a privacy interest in location data. The Fifth and Eleventh Circuits decided that individuals have no privacy interest in their location information over long term tracking. But the D.C. Circuit concluded the opposite. *United States v. Maynard*, 615 F.3d 544, 562-63 (D.C. Cir. 2010). Similarly, the Third Circuit explained that CSLI can locate a person inside

private space, like a home, which implicates a privacy interest long recognized by the Fourth Amendment. *In re Application (Third Circuit)*, 620 F.3d at 311-13 (explaining that CSLI allows the government to see inside a home, which is government surveillance that requires a warrant) (relying on *United States v. Karo*, 468 U.S. 705 (1984)). Moreover, the supreme courts of Florida and Massachusetts and the Court of Appeals of New York all recognize that individuals enjoy a privacy interest in their location information. *Commonwealth v. Augustine*, 4 N.E.3d 846, 864 (Mass. 2014); *Tracey*, 152 So. 3d at 525; *People v. Weaver*, 909 N.E.2d 1195, 1201 (N.Y. 2009).

These splits existed before the panel's decision. The panel thoroughly addressed all the different positions in its 134-page opinion. If any further review of this issue should occur, it should be in the Supreme Court, the only forum that can clarify the fractured state of the law. A petition for certiorari is already pending in *Davis*, which, if granted, would resolve these splits.

II. The panel decision is consistent with *Miller* and *Smith*.

The government argues that the panel's decision cannot be reconciled with *United States v. Miller* and *Smith v. Maryland* because individuals disclose their location information to third parties, who then maintain it as a business record. (Pet. at 7.) The government is wrong; the panel's decision is entirely consistent with

Miller and *Smith*.

The government reads *Miller* and *Smith* in the broadest possible terms, inferring a holding that establishes an absolute rule that any type of information, no matter how private, that a third party maintains enjoys no Fourth Amendment protection. *Miller* and *Smith*, however, held no such thing. And more important, numerous cases in the ensuing forty years recognize a constitutionally protected privacy interest in information disclosed to and held by third parties.

Miller reiterated what the Court stated in *Katz v. United States*, 389 U.S. 347 (1967): the Fourth Amendment does not protect "'what a person knowingly exposes to the public.'" 425 U.S. at 42 (quoting *Katz*, 389 U.S. at 351). This statement, however, does not encompass the entire holding of *Miller*. The Court explained that "We must examine the nature of the particular documents sought to be protected to in order to determine whether there is a legitimate expectation of privacy concerning their contents." *Id.* In *Miller*, the documents were "not confidential communications but negotiable instruments." *Id.* The nature of the record thus demonstrated that the individual did not have an objectively reasonable expectation of privacy.

Smith likewise reaffirmed *Katz's* holding that individuals do not maintain "a legitimate expectation of privacy in information [they] voluntarily turn[] over to third parties." 442 U.S. at 743-44. The Court decided that an individual voluntarily

discloses to a telephone company the telephone numbers that he or she dials. Two facts played a key role in the Court's decision. First, the information that the government obtained is "limited." *Id.* at 742. Second, the telephone user "voluntarily convey[s] numerical information to the telephone company" when dialing a telephone number. *Id.* at 744. The limited information that the land-line telephone user disclosed to the telephone company is the only information that the government obtained. The telephone user knew precisely what that information was and could control whether it was revealed or not. Indeed, the user saw a print out of the numbers in each monthly bill.

The panel's decision is consistent with both cases. These cases establish that information that individuals disclose to third parties may be available to the government if the disclosure is voluntary, the information is limited, and the nature of the information or documents is not inherently private. The records at issue in *Miller* and *Smith* conveyed limited information to the business, the individual knew precisely what information he was conveying, and the individual could control the flow of information. The information was tangible and visible to the individual.

But CSLI exposes vast amounts of private information even when individuals take no affirmative steps to disclose their location data to the public. CSLI is generated automatically and passively, without any choice or overt action by the cell

phone user, including when the user is not even making or receiving calls. Unlike the records in *Miller* and *Smith*, individuals do not know precisely when a phone is passively conveying location data, or to which cell tower the phone is connecting.

FBI experts concede that CSLI can locate a citizen and her property, including within the home, whenever a cell phone is turned on, without the user's input or control: "'CSLI for a cellular telephone may still be generated in the absence of user interaction with a cellular telephone. ... For example' the CSLI may be generated by 'applications that continually run in the background that send and receive data (e.g. mail applications).'" *In re Application*, __ F. Supp. 3d __, 2015 WL 4594558 *13 (N.D. Cal. 2015) (quoting the declaration of FBI Special Agent Hector M. Luna); *see also id.* at *9. Here, the record establishes that CSLI was generated when the defendants were *not* actively using their cell phones. (JA 1974, 1980, 1992.)

The choices that the defendants in *Smith* and *Miller* made, to disclose limited, specific information to businesses, evinced a lack of interest in maintaining privacy. Since cell phone users, in contrast, make no active, deliberate choice to reveal the nature and scope of information encompassed in CSLI, they retain their privacy interest. The simple act of carrying a cell phone does not indicate a disinterest in maintaining privacy. *See Weaver*, 909 N.E.2d at 1200 ("It would appear to us that the great popularity of . . . technology for its many useful applications may not be taken

simply as a massive, undifferentiated concession of personal privacy to agents of the state."). Thus, the panel's decision does not conflict with *Smith* and *Miller*, but applies the cases consistently with the cases' own internal limitations.

Moreover, although the government does not mention any third party cases decided after 1979, later Supreme Court cases hold that the Fourth Amendment applies to information revealed to third parties. (*See* Pet. at 7-10.) For example, in *Ferguson v. City of Charleston*, 532 U.S. 67 (2001), the Court rejected the government's argument that patients lose a privacy interest in sensitive information once they share it with another. "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests . . . is that the results . . . will not be shared with nonmedical personnel without her consent." *Id.* at 78. Although the documentation of the drug tests was created and maintained by a hospital, the individual maintained a constitutionally protected privacy interest in the information. *Id.* Likewise, in *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010), the Court assumed that police officers retained a privacy interest in text messages sent on government-owned and monitored pagers, but found that a different exception to the warrant requirement authorized the search. Not only did the telecommunications provider retain this information, but the police department itself monitored the text messages. The Court had no qualms about the existence of the privacy interest

despite this access by third parties. *See also Bond v. United States*, 529 U.S. 334, 336 (2000) (rejecting the government's third party argument and concluding that passengers on common carriers retain a privacy interest in carry-on luggage, although others might see and even touch it).

This Court's more recent third party jurisprudence is consistent with *Ferguson* and *Quon*. In *Doe v. Broderick*, this Court found a Fourth Amendment privacy interests in information and documents containing private information held by third parties – a patient's file from a methadone clinic. 225 F.3d 440, 450-52 (4th Cir. 2000). When law enforcement examined that file without a warrant or probable cause, it constituted an unreasonable search under the Fourth Amendment. *Id.*

In its request to rehear this case, the government ignores cases addressing private information in a third party's hands, if they were decided after 1979. But these later cases demonstrate that when third parties maintain records of an individual's highly private information, that private information still enjoys protection from the government's prying eyes, unless the government produces a warrant based on probable cause. The panel rightly continued reading cases that were decided after *Smith*. As a result, the panel reached a conclusion that is both consistent with *Smith* and *Miller*, and is in line with more recent third party cases. The individuals in those cases did not forfeit a privacy interest in their sensitive

information simply because a business or individual had access to that information. The panel correctly concluded that the defendants here did not forfeit their privacy interests in their CSLI.

III. The decision is consistent with cases recognizing a privacy interest in location information.

The government offers a different iteration of its same third-party doctrine argument, claiming that cases addressing long term location monitoring are irrelevant because this case does not involve "direct tracking." (Pet. at 4, 10.) The panel's decision, however, is correct.

Riley v. California establishes that individuals have a privacy interest in historical CSLI. 134 S. Ct. 2473, 2490 (2014). Historical CSLI generated by cell phones served as one of the Court's chief examples of "the privacies of life" included in cell phone metadata. The Court described just how intimate and detailed location data is: "Data on a cell phone can also reveal where a person has been. Historic location information . . . can reconstruct someone's specific movements down to the minute, not only around town, but within a particular building." *Id.* The Court explained the intrusive nature of CSLI tracking by adopting Justice Sotomayor's concurrence in *United States v. Jones*, 132 S. Ct. 945, 955 (2012). The unanimous *Riley* Court thus concluded that monitoring "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" infringes upon an individual's reasonable expectation of a privacy that is protected by the Fourth Amendment. *Id.*

The government's position that people cannot have a privacy interest in historic CSLI thus directly opposes what a unanimous Supreme Court decided a little more than a year ago. The panel, on the other hand, followed Supreme Court guidance and recognized a privacy interest in historic CSLI.

The conclusions in *Riley* (as well as the panel's) flow logically from *United States v. Karo*, 468 U.S. 705 (1984), and *Kyllo v. United States*, 533 U.S. 27 (2001). Those cases establish that individuals have a reasonable expectation of privacy in details about the interior of private space, like a home, including who or what is inside. *Kyllo*, 533 U.S. at 34. The government may not track a person or his effects inside a home without a warrant: "private residences are places in which the individual normally expects privacy free of government intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Karo*, 468 U.S. at 714; *see also Kyllo*, 533 U.S. at 40 (holding that the Fourth Amendment draws a "firm" and "bright line" at the entrance to a house). Unless the police have a warrant, they may not use technology to observe details about the interior of a person's home that are otherwise invisible without a physical

intrusion into the constitutionally protected area. *Id.* *See also Karo*, 468 U.S. at 715-16; *Jones*, 132 S. Ct. at 953. And CSLI allows the government to observe a citizen, together with his or her personal property, in private space. *See Riley*, 134 S. Ct. at 2490; *In re Application (Third Circuit)*, 620 F.3d at 311-13; *Augustine*, 4 N.E.3d at 864; *Tracey*, 152 So. 3d at 525.

The government is mistaken in its claim that the third party doctrine renders these cases inapplicable. (Pet. at 10-11.) *Miller* and *Smith* simply provide a second step in the analysis of whether the government is intruding upon an individual's reasonable expectation of privacy. Location tracking cases are essential to the Fourth Amendment analysis, providing the necessary first step. Courts cannot examine the "nature of the record" under *Miller* and *Smith*, let alone whether a citizen has voluntarily shared that information with a third party without first determining the privacy interest at stake. *Riley*, *Kyllo*, *Karo*, and even *Jones* establish that CSLI is private on a level far surpassing anything involved in *Smith* and *Miller*.

Just like the government stopped reading third party cases dating after 1979, it asks the Court to skip the initial step in the Fourth Amendment analysis. This logical leap is necessary to the government's argument, because a head-on analysis of these cases compels the conclusion that historical CSLI remains private and falls into a category unlike bank records or dialed phone numbers. The panel, however,

followed the proper analytical steps: it determined the nature of the information at issue, considered the privacy implications of that record, and then decided whether cell phone users knowingly and voluntarily convey that information to third parties. The government posits that *Smith* and *Miller* are the only relevant cases, but the panel correctly decided that courts cannot divorce the nature of the record from the Fourth Amendment calculus.

IV. The government's argument that the panel decision altered the reasonableness requirement for subpoenas is really another restatement of its argument about *Miller* and *Smith*.

Finally, the government suggests that this Court should rehear this case because subpoenas, supported by reasonable suspicion, and 18 U.S.C. § 2703(d) act as an exception to the warrant requirement. (Pet. at 12.) The government also asserts that the panel imposed a probable cause standard onto subpoenas. The government is wrong on both counts.

Subpoenas are not an exception to the warrant requirement, but simply fall outside the warrant clause. Unlike a search, which requires a warrant and probable cause, a subpoena begins an adversary process, where the parties are able to litigate the reasonableness of the government' request before complying. *In re Subpoena Duces Tecum*, 228 F.3d 341, 348 (4th Cir. 2000). The intrusion into a recognized privacy interest is far more limited than in a search. *Id.* A subpoena thus is not an

exception to the warrant requirement; it simply is not a warrant.[3]

The issue the panel had to decide, and decided correctly, was whether collecting and analyzing CSLI is a search. Courts decide whether a particular governmental investigation technique is a search using the two-part test outlined in *Katz v. United States*, 389 U.S. 347 (1967). *See also Jones*, 132 S. Ct. at 949, 953 (holding that although a search certainly occurs when the government commits a common law trespass, "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."). First, a court assesses whether the privacy interest upon which the government seeks to intrude is one that society accepts as objectively reasonable. Second, the court determines whether the individual's expectation of privacy is subjectively reasonable. *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring).

Having conducted the *Katz* analysis, the panel concluded that collecting and analyzing CSLI is indeed a search. Given the substantial privacy interests implicated by the government's analyzing of location data over a seven-month period, as discussed above, this conclusion was both correct and consistent with decisions of the Supreme Court and several states' highest courts. Therefore, because what happened

[3] Indeed, a court order under § 2703(d) operates like a warrant, not a subpoena. It is issued under seal, with a gag order, providing no adversary process for the cell phone user to challenge the search until after criminal proceedings begin.

was a search, the Fourth Amendment's warrant requirement applies. *See In re Subpoena Duces tecum*, 228 F.3d at 348 (searches remain subject to the warrant requirement).

The panel's decision does not overrule Circuit precedent regarding reasonableness requirements for subpoenas. (Pet. at 12.) Leaving subpoena standards unchanged, the panel's decision concludes that the government activity here fell under the warrant requirement.

CSLI is not immune from search. The government just must seek a warrant, something the Stored Communications Act itself contemplates. 18 U.S.C. § 2703(c). "Our cases have historically recognized that the warrant requirement is an important part of the our machinery of government, not merely an inconvenience to be somehow weighed against the claims of police efficiency." *Riley*, 134 S. Ct. at 2493 (internal quotation omitted).

Conclusion

The panel's decision correctly applied Supreme Court case law. It is consistent with decisions from other circuits and several states' supreme courts. Although the panel's decision conflicts with decisions from the Fifth and Eleventh Circuits, rehearing would not resolve this split. This Court should therefore deny the government's petition for rehearing.

Respectfully submitted,

JAMES WYDA
Federal Public Defender

_____/s/_____
MEGHAN S. SKELTON
Appellate Attorney
6411 Ivy Lane, Ste. 710
Greenbelt, Maryland 20770
(301) 344-0600

CERTIFICATE OF COMPLIANCE

1. This Opposition to the Government's Petition for Rehearing has been prepared using WordPerfect X4 software, Times New Roman font, 14 point proportional type size.

2. Exclusive of the table of contents, table of authorities, and certificate of service, this brief contains 15 pages.

I understand that a material misrepresentation can result in this Court's striking the brief and imposing sanctions. If the Court so requests, I will provide an electronic version of the brief and/or a copy of the word or line print-out.

10/06/15
Date

/s/ Meghan S. Skelton
Meghan S. Skelton
Appellate Attorney

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 6th day of October, 2015 a copy of the foregoing Opposition to the Government's Petition for Rehearing En Banc was delivered via electronic filing to:

Sujit Raman, Esq.
Assistant U.S. Attorney
Office of the U.S. Attorney
6500 Cherrywood Lane, Suite 200
Greenbelt, Maryland 20770

_____/s/_____
Meghan S. Skelton
Appellate Attorney