No. 12-4659 (L)

IN THE UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

UNITED STATES OF AMERICA,

Appellee,

v.

AARON GRAHAM
and
ERIC JORDAN,

Appellants.

Appeal from the United States District Court for the
District of Maryland, Northern Division
Honorable Richard D. Bennett, District Judge

GOVERNMENT'S PETITION FOR REHEARING EN BANC

Rod J. Rosenstein
United States Attorney

Sujit Raman
Chief of Appeals

Nathan Judish
Attorney, Computer Crime &
Intellectual Property Section,
U.S. Department of Justice

6500 Cherrywood Lane, Suite 200
Greenbelt, Maryland 20770
(301) 344-4433

Attorneys for the Appellee

September 17, 2015

TABLE OF AUTHORITIES

CASES

Statutes

Rules

INTRODUCTORY STATEMENT

The panel decision struck down Section 2703 of the Stored Communications Act on the theory that the statute unconstitutionally authorizes courts to issue orders for historical cell-site location information (CSLI) from communications providers. Its reasoning "flies in the face of the Supreme Court's well-established third-party doctrine," Op. 106 (Motz, J., dissenting), by contravening *United States* v. *Miller*, 425 U.S. 435 (1976), and *Smith* v. *Maryland*, 442 U.S. 735 (1979). Its logic "lacks support from all relevant authority and places [this Court's jurisprudence] in conflict with the Supreme Court and three other federal appellate courts." Op. 114; *see United States* v. *Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re Application of the United States*, 724 F.3d 600 (5th Cir. 2013); *In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). Its holding disregards the precedent of this Court and the Supreme Court regarding the reasonableness requirement for compulsory process. *See In re Subpoena Duces Tecum*, 228 F.3d 341, 346-49 (4th Cir. 2000); *United States v. R. Enterprises*, 498 U.S. 292, 297 (1991). The decision "is a constitutional outlier—untenable in the abstract and bizarre in practice," which "will have profound consequences in future cases." Op. 126, 106 n.1.

En banc review is therefore necessary to avoid conflict with the Supreme Court's decisions (and those of other circuits); to maintain the uniformity of this Court's decisions; and to address a question of exceptional importance.

QUESTION PRESENTED

Whether the government's acquisition of historical cell site records from a third-party telecommunications provider pursuant to a court order issued in compliance with 18 U.S.C. § 2703(d) violates the Fourth Amendment.

STATEMENT OF THE CASE

1. Defendants Aaron Graham and Eric Jordan were indicted in the District of Maryland for committing a series of armed robberies in and around Baltimore in early 2011. Thirty-nine witnesses testified in the government's case-in-chief, and prosecutors introduced more than 200 physical exhibits in the form of photographs, videos, clothing, firearms, ammunition, reports and records, latent print cards, maps, and stipulations. Gov't Br. 35. Two cell phones were seized from Graham and Jordan, and the government also introduced records obtained from Sprint/Nextel showing which cell towers those phones used to make or receive calls and text messages at times relevant to the robberies. The jury convicted both defendants of all charges, and the district court sentenced Graham and Jordan to 147 years and 72 years of imprisonment, respectively. The defendants timely appealed.

2. The Stored Communications Act (SCA), 18 U.S.C. §§ 2701-2712, authorizes a court to issue an order compelling a service provider to disclose non-content records of electronic communications if the government "offers specific

and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . sought[] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Here, the government sought two separate § 2703(d) orders for information about which cell towers the phones had used. The first order issued in March 2011 and covered four specific time periods between August 2010 and February 2011, totaling 14 days, linked to particular robberies. Gov't Br. 25. The second order issued four months later, after the government obtained information about other similar and possibly related robberies, and sought historical CSLI from July 1, 2010 through February 6, 2011. Gov't Br. 26.

3. The defendants moved to suppress the historical CSLI on Fourth Amendment grounds. The district court rejected their claim based on the third-party doctrine: "Like the bank records at issue in *Miller*, the telephone numbers dialed in *Smith*, and the subscriber information collected in [*United States* v.] *Bynum* [604 F.3d 161 (4th Cir. 2010)], historical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers." *United States* v. *Graham*, 846 F. Supp. 2d 384, 400 (D. Md. 2012).

4. This Court affirmed the defendants' convictions, but the majority opinion held that the government violated the Fourth Amendment by obtaining historical CSLI with a § 2703(d) order. Op. 1, 13-65. The majority ruled that cell-phone users have an objectively reasonable expectation of privacy in a phone company's

historical CSLI, in part because such information "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." Op. 19. The majority held that the government conducts a Fourth Amendment search whenever it obtains third-party records of historical CSLI "pertaining to an extended time period like 14 or 221 days." Op. 32; *see* Op. 19. The point between zero and 14 days at which obtaining cell-site records becomes a search remains unclear.

In reaching this conclusion, the majority (1) analogized the government's examination of historical CSLI to the searches in *United States* v. *Karo*, 468 U.S. 705 (1984), and *Kyllo* v. *United States*, 533 U.S. 27 (2001), which involved the government's direct tracking of suspects, rather than the inspection of third-party business records, and (2) focused on what such information might allow the government to learn, rather than on how the information was obtained. *See* Op. 24. Although this case involved no precise location information, no trespass, and no real-time monitoring by the government, the majority held that the privacy concerns regarding "longer term GPS monitoring" raised by five concurring Justices in *United States* v. *Jones*, 132 S. Ct. 945 (2012), applied "with equal or greater force" to historical CSLI. Op. 27. The majority opined that the government's inspection of historical CSLI invaded privacy interests because "track[ing]" cell phones using such data relies "upon technology not in general use to discover the movements of

an individual over an extended period of time." Op. 31. The majority also rejected the district court's holding that the CSLI used in this case was not sufficiently precise or continuous to raise privacy concerns. Op. 32-36.

The majority flatly rejected application of the third-party doctrine. Op. 36-60. The majority sought to distinguish *Miller* and *Smith* on the ground that "the defendant in those cases had 'voluntarily conveyed' the information to the third party." Op. 39; *see* Op. 42-43. The majority concluded that historical CSLI is not "voluntarily conveyed" because a "user is not required to actively submit any location-identifying information when making a call or sending a message." Op. 44. Disregarding the undisputed evidence that cell phones cannot work unless the service provider knows which cell tower to use, and that Sprint/Nextel informed customers that it collected their location information, the majority deemed it "clear" that "cell phone users do not voluntarily convey their CSLI to their service providers." Op. 20, 39, 40-45. Evidence that customers know that their phone must connect with a service provider's nearby tower was "beside the point," the majority found, because users generally are not aware of which specific cell tower their phone uses to connect to a cellular network. Op. 48; *see* Op. 48-51.

The majority rejected suppression because the government obtained the CSLI in good-faith reliance on court orders. Op. 60-65. The majority ruled, however, that the good-faith exception would not be available to the government in future cases

presenting the same issue. Op. 65 n.25.[1] Judge Thacker joined the majority opinion by Senior Judge Davis and filed a concurrence to express her "concern about the erosion of privacy in this era of rapid technological development." Op. 102.

5. Judge Motz dissented from the majority's Fourth Amendment holding. Op. 106-34. As she recognized, "[i]t matters, for Fourth Amendment purposes, *how* the government acquires information." Op. 108 n.2 (emphasis in original). Because Sprint/Nextel obtained the information for its own purposes in the normal course of business, Judge Motz distinguished the surreptitious government activity in *Karo*, *Kyllo*, and *Jones*, and instead applied the third-party doctrine. Op. 107-11, 128-30. Moreover, Judge Motz noted, there is "little question" that cell-phone users reveal their locational information to their service providers and do so voluntarily, as that term is normally understood in the Fourth Amendment context. Op. 115-18. Judge Motz also took issue with the majority's suggestion that the third-party doctrine applies only when a user "actively submits" information, noting that "such a rule is nowhere to be found in either *Miller* or *Smith*" and is inconsistent with circuit precedent and the decisions of other courts of appeals. Op. 119; *see* Op.

[1] For this reason, and because the majority opinion limits the government's ability to obtain § 2703(d) orders in future investigations, the government seeks rehearing en banc even though the defendants' convictions were affirmed. *See* Fed. R. App. 35(b) (providing that "[a] party may petition for hearing or rehearing en banc," and omitting any exception for prevailing parties); *United States* v. *Davis*, 573 Fed. Appx. 925 (11th Cir. 2014) (granting government en banc petition in analogous context).

118-22. Finally, Judge Motz observed that the Supreme Court may revisit the third-party doctrine, but only the Supreme Court can overrule it. Op. 133-34.

REASONS FOR GRANTING THE PETITION

1. The majority's holding that the defendants "have a reasonable expectation of privacy in their long-term CSLI," Op. 58-59, cannot be reconciled with *United States* v. *Miller*, 425 U.S. 435 (1976), and *Smith* v. *Maryland*, 442 U.S. 735 (1979). Those cases establish that an individual has no expectation of privacy in information conveyed to and maintained by a third party for its own business purposes. That principle squarely applies to CSLI records maintained by and obtained from a cell-phone provider.

a. The Supreme Court "has repeatedly held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 443). In *Miller*, the Court held that bank customers have "no protectable Fourth Amendment interest" in "the business records of the banks" (including checks, deposit slips, and financial statements)—records that a federal statute required the banks to maintain. 425 U.S. at 436-38, 441-42. Similarly, the *Smith* Court held that a phone customer lacks a legitimate expectation of privacy in the numbers dialed from his phone. 442 U.S. at 744-46. Those holdings are consistent with the plain text of the Fourth Amendment, which protects "[t]he right of the people to be secure in *their*

. . . papers, and effects" (emphasis added), not the records of *others*. Accordingly, "the government . . . does not engage in a Fourth Amendment 'search' when it acquires [business records] from a third party." Op. 110 (dissent).

Like the bank customer in *Miller* and the phone customer in *Smith*, the defendants sought to suppress business records over which they could "assert neither ownership nor possession." *Miller*, 425 U.S. at 440. The historical CSLI records "pertain[ed] to transactions to which [Sprint/Nextel] itself was a party," *id*. at 441; were generated "for its own business purposes," *In re Application*, 724 F.3d at 611-12; were stored on its premises; and were subject to its control.

The majority erred in concluding that the defendants had a subjective expectation of privacy in Sprint/Nextel's records because "cell phone users do not voluntarily convey their CSLI to their service providers." Op. 39. Disclosure of CSLI is voluntary. As Judge Motz explained, cell-phone users know that their phones emit signals that are conveyed to service providers, through facilities close to their phone, as a necessary incident of making or receiving calls. Op. 115-17. In addition, Sprint/Nextel informed customers that it would collect their location information. Op. 20. Here, the defendants also tried to conceal their connections to the phones, which further demonstrates that they expected their phones to convey incriminating information to third parties. Op. 54 & n.20. The defendants "cannot

now protest that providing this essential information was involuntary." Op. 118.[2]

As Judge Motz observed, the majority's insistence that an individual only "voluntarily conveys" what he "actively submits" contravenes long-established business records jurisprudence. *See* Op. 119-20. Customers do not "actively submit" the date, time, and duration of phone calls, but neither this Court nor any other court has held that such information is protected by the Fourth Amendment. The majority's reasoning could have far-reaching consequences. For example, Internet communications are routed via IP address, and courts have held that users lack a reasonable expectation of privacy in IP address information, *see, e.g.*, *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)—but users do not actively submit IP addresses to their service providers. The majority's creation of a Fourth Amendment interest in such data vitiates the third-party doctrine and eliminates the bright line (or any discernable line at all) between information protected by the

[2] Even if the defendants did not voluntarily disclose CSLI, the third-party doctrine is not limited to information voluntarily disclosed by a defendant. When a witness collects and retains its own information without state action, the government may obtain the witness's information regardless of whether the information was voluntarily conveyed to the witness. The Supreme Court addressed voluntariness in *Miller* and *Smith* because the bank was required by law to maintain the records, and the phone company acted as a government agent in monitoring the defendant at the government's request. 425 U.S. at 441; 442 U.S. at 739 n.1. Whether information has been voluntarily disclosed plays no role in business records cases *not* involving state action. *See, e.g.*, *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 & n.11 (1984) (financial records in absence of data retention law); *Donaldson v. United States*, 400 U.S. 517, 522 (1971) (employment records); *First Nat. Bank of Mobile v. United States*, 267 U.S. 576 (1925) (bank records prior to data retention law).

Fourth Amendment and information that belongs to a third-party.

Even if the defendants were unaware that the service provider needs to know which tower to use, such subjective ignorance cannot be *objectively* reasonable. Wireless phones free the customer from the need to connect to a network with a stationary cord, but they do not free the customer from the need to connect to a network. When the third-party provider makes a record of which cell tower it uses to make service available to the customer, that record does not infringe the customer's rights. *See Smith*, 442 U.S. at 745 (stating that the "fortuity of whether or not the phone company in fact elects to make a quasi-permanent record" of information does not "make any constitutional difference"). Consistent with the third-party doctrine, no Fourth Amendment search takes place when the government obtains a provider's CSLI under under § 2703(d) because a person has no constitutional expectation of privacy in business records owned by a third party.

b. *Karo*, *Kyllo*, and *Jones* do not exempt location information from the third-party doctrine. As Judge Motz observed, the majority misread *Karo* and *Kyllo* to support the abstract proposition that an individual has an expectation of privacy in his location and movements over time. But those cases actually "involve[d] direct surveillance," *i.e.*, real-time tracking of a particular person *by government agents* in their homes and other places, and therefore concerned "the right of the people" to be "secure in their persons, houses, . . . and effects," U.S. Const., Amend. IV, from

government efforts to "surreptitiously collect private information." Op 109, 108. Here, by contrast, the government did not engage in any surveillance at all. Instead, it simply collected historical information from a witness (the phone company), which the witness compiled and maintained in the ordinary course of business.

Likewise, *Jones* has no application here. This case involves no physical incursion into a constitutionally-protected area. Officers in *Jones* did not obtain location data from a third-party service provider, and the Court did not discuss the third-party doctrine. And while one concurring Justice in *Jones* suggested that the Supreme Court should reconsider its third-party rule, even she did not suggest that *other courts* are not bound by that rule in the interim. *See* 132 S. Ct. at 957 (Sotomayor, J.). Moreover, four of the five concurring Justices went out of their way in *Jones* to encourage legislative solutions of the kind struck down in this case. *See id.* at 964 (Alito, J., concurring) ("In 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.").

2. In a footnote, the majority held that § 2703(d) orders for CSLI not only implicate a reasonable expectation of privacy, but also violate the Fourth Amendment because they "do not fit within any of the 'well delineated exceptions'" to the warrant requirement. Op. 20 n.2 (rejecting *Davis*'s holding that use of

Section 2703(d) orders to obtain historical CSLI is reasonable). But there *is* a long-established exception to the warrant requirement applicable here: A § 2703(d) order is a judicial subpoena, and this Court has held that subpoenas "are limited by the general reasonableness standard of the Fourth Amendment (protecting the people against "unreasonable searches and seizures"), not by the probable cause requirement." *In re Subpoena Duces Tecum*, 228 F.3d at 348. The rule that subpoenas are subject only to a reasonableness requirement is deeply rooted in Supreme Court precedent. *See, e.g.*, *R. Enterprises*, 498 U.S. at 297 (rejecting probable cause requirement for subpoenas because "the very purpose of requesting the information is to ascertain whether probable cause exists"); *Kastigar v. United States*, 406 U.S. 441, 443 (1972) (stating that the government's right to every person's evidence through compulsory process "was considered an 'indubitable certainty' that 'cannot be denied' by 1742"); *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946) (holding that subpoenas under the Fourth Amendment are subject "at most" to a reasonableness requirement).

More careful consideration than a summary footnote is warranted before this Court strikes down § 2703(d) as it applies to cell-site records; overrules precedent regarding the Fourth Amendment requirements for subpoenas; creates a circuit split with *Davis* regarding whether use of § 2703(d) orders to obtain CSLI is reasonable under the Fourth Amendment; and creates enormous uncertainty over the use of

compulsory process to obtain business records. This Court should not hold that Section 2703(d) orders are unconstitutional without carefully evaluating whether § 2703(d) satisfies the core reasonableness requirement of the Fourth Amendment.

As the Eleventh Circuit recognized, Congress did not "lower the bar from a warrant" in enacting § 2703(d); instead, "requiring a court order under § 2703 raises the bar from an ordinary subpoena to one with additional privacy protections built in." *Davis*, 785 F.3d at 505-06. Congress went well beyond the constitutional prerequisites for obtaining third-party business records by: (1) requiring prior approval of a neutral and detached magistrate; (2) authorizing the judicial officer to act only if specific and articulable facts establish reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation; and (3) prohibiting improper disclosures of the records. *See* §§ 2703(d), 2707(g). The majority failed to apply the "strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is 'reasonable'" within the meaning of the Fourth Amendment. *United States* v. *Watson*, 423 U.S. 411, 416 (1976). In sum, § 2703(d) satisfies an established exception to the warrant requirement, and it is more protective of individual privacy than other commonly accepted and practically indistinguishable forms of compulsory process.

3. The majority's holding also conflicts with the en banc Eleventh Circuit's decision in *Davis*, the Fifth Circuit's decision in *In re Application*, and the Third

Circuit's holding in its *In re Application*, each of which upheld § 2703(d) against a Fourth Amendment challenge. Moreover, the vast majority of federal district courts have rejected the majority's reasoning. *See* Op. 112-14. The majority made little effort to reconcile its holding with the conflicting circuit court opinions, simply declaring that those cases applied the third-party doctrine too expansively. But the majority's reasoning is unpersuasive for the reasons Judge Motz has well explained, and it creates a circuit split with serious implications for law enforcement.

4. The panel's ruling substantially burdens important governmental interests. Law-enforcement agencies rely on CSLI to investigate and solve serious crimes in which they lack probable cause to obtain a warrant but reasonably believe that the requested records will be of use. Investigators use CSLI early in investigations as a building block to develop probable cause for search warrants, and in other investigations they use CSLI to connect dots and solve crimes that might otherwise go unsolved. In such cases, § 2703(d) orders—like other forms of compulsory process not subject to the warrant requirement—help deflect suspicion from the innocent, build probable cause against the guilty, aid in the search for truth, and conserve scarce investigative resources.[3]

[3] The majority's refusal to draw a "bright line" as to when the Fourth Amendment is implicated in this context is eliminating the use of § 2703(d) orders to obtain historical cell-site records. Magistrates in Maryland already have simply defaulted up to the warrant requirement—contrary to Congress's clearly articulated wishes.

Those real-world benefits come at a negligible cost to individual privacy. Unlike real-time tracking, historical cell-site records contain information already known and used by third parties. Unlike GPS data, CSLI does not provide precise location information; its precision in this case was on the order of miles. *See* Op. 35 n.11. Such general location information does not reveal sensitive or private activities and is useful only if police already have a point of reference, such as a robbery location. Finally, any information theoretically discoverable from such records is subject to statutory safeguards crafted to avoid unwarranted invasions of individual privacy. Those protections amply accommodate any diminished expectation of privacy the defendants may assert in Sprint/Nextel's records.

CONCLUSION

The panel decision should be vacated and the petition for rehearing en banc should be granted.

Respectfully submitted,

Rod J. Rosenstein
United States Attorney

/s/
Sujit Raman
Chief of Appeals
District of Maryland

September 17, 2015

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on September 17, 2015, I electronically filed the foregoing with the Clerk of Court using the CM/ECF System, which will send notice of such filing to all registered counsel of record.

/s/
Sujit Raman
Assistant United States Attorney