No. 12-12928-UU

IN THE

United States Court of Appeals

FOR THE ELEVENTH CIRCUIT

UNITED STATES OF AMERICA,
Appellee,

v.

QUARTAVIOUS DAVIS,
Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

EN BANC BRIEF OF THE UNITED STATES OF AMERICA

WIFREDO A. FERRER
UNITED STATES ATTORNEY

KATHLEEN M. SALYER
CHIEF, APPELLATE DIVISION

AMIT AGARWAL
ASSISTANT UNITED STATES ATTORNEY

U.S. ATTORNEY'S OFFICE
SOUTHERN DISTRICT OF FLORIDA
99 N.E. 4TH STREET
MIAMI, FLORIDA 33132
(305) 961-9425

Attorneys for Appellee

***United States v. Quartavious Davis*, Case No. 12-12928-UU**

Certificate of Interested Persons

Undersigned counsel for the United States of America hereby certifies that the Certificate of Interested Persons set forth in Davis's brief included a complete list of persons and entities who have an interest in the outcome of this case.

/s/ *Amit Agarwal*
Amit Agarwal
Assistant United States Attorney

Table of Contents

Page:

Table of Contents

(continued)

Page:

Table of Contents

(continued)

Page:

Table of Contents

(continued)

Page:

Table of Citations

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Table of Citations (Continued)

Cases: **Page:**

Statutes & Other Authorities: **Page:**

Table of Citations (Continued)

Statutes & Other Authorities: **Page:**

Statement of Jurisdiction

This is an appeal from a final judgment of the United States District Court for the Southern District of Florida in a criminal case. The district court entered judgment against appellant Quartavious Davis on May 17, 2012 (DE342).[1] The district court had jurisdiction to enter the judgment pursuant to 18 U.S.C. § 3231. Davis filed a timely notice of appeal on May 29, 2012 (DE344). *See* Fed. R. App. P. 4(b). This Court has jurisdiction over this appeal pursuant to 28 U.S.C. § 1291 and 18 U.S.C. § 3742(a).

[1] Unless otherwise noted, all record citations included in this brief refer to the underlying criminal case, SDFL Case No. 10-cr-20896. Record materials are cited by docket entry number (DE) or government exhibit number (GX). Where appropriate, the page number of the document in question is listed after a colon following the DE or GX number.

Statement of the Issues

1. Whether the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), is unconstitutional under the Fourth Amendment insofar as it authorizes the government to acquire records showing historical cell site location information from a telephone service provider.

2. On the facts of this case, whether the government acquisition, pursuant to a court order authorized by the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), of cellular telephone records showing historical cell site location information from a telephone service provider constitutes an unreasonable search or seizure in violation of Davis's constitutional rights under the Fourth Amendment.

Statement of the Case

1. Course of Proceedings

A federal grand jury sitting in the Southern District of Florida returned a superseding indictment charging appellant Quartavious Davis and five codefendants with various offenses arising out of seven armed robberies (DE39). Davis filed a motion to suppress certain historical cell tower records produced by MetroPCS (DE272). The district court denied that motion (DE277:45), the jury convicted Davis on all counts (DE293), and Davis was sentenced to a prison term of 1,941 months (DE342).

A three-judge panel of this Court concluded that the government violated Davis's rights under the Fourth Amendment by obtaining cell tower records from a third-party service provider pursuant to a non-warrant court order issued under the Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d). *United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014). Nevertheless, the panel affirmed Davis's convictions based on the good-faith exception to the exclusionary rule. *Id.* at 1217-18. This Court vacated the panel's decision and granted the government's petition for rehearing en banc. *United States v. Davis*, 573 F. App'x 925 (2014).

2. Factual & Procedural Background

A. Offense Conduct

Over a two-month period in 2010, Davis and various accomplices committed seven armed robberies in South Florida. At trial, the government presented testimony from two accomplices, Willie Smith and Michael Martin (DE279:201-34; DE281:5-99; DE283:85-202). Smith and Martin testified that Davis participated in the seven robberies, described how those robberies were carried out, and identified Davis as one of the robbers depicted on certain security surveillance videos (*id*). Two eyewitnesses, Edwin Negron and Antonio Brookes, also testified to Davis's role in two of the robberies (DE281:170-81; DE283:69-84). Davis's DNA was recovered from two of the getaway cars used by the robbers (DE283:26-69). Records obtained from MetroPCS showed that, for six of the seven crimes, cellular telephones used by Davis and his accomplices made and/or received calls in the vicinity of the robbery at or near the time of the offense (DE283:204-237; DE285:19-52).

B. Issuance of the 2703(d) Order

During the course of its investigation, the government applied to a federal magistrate judge for a court order directing various phone companies to disclose non-content toll records for four subject telephone numbers, along with "the

corresponding geographic location (cell site) data relating to the Subject Lines captured by the wire communication provider" (DE268-1:6). The application was submitted pursuant to the Stored Communications Act (SCA), 18 U.S.C. § 2701 *et seq.*, which provides that a federal or state governmental entity may require a telephone service provider to disclose non-content subscriber records if a court of competent jurisdiction finds "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." *Id.* § 2703(c)(1)(B), (d). The government did not seek or obtain either GPS or real-time (also known as "prospective") location information (DE268-1:6; DE277:9). Nor did it seek data specifying the location of Davis's cell phone. Instead, it requested historical "cell site" (i.e., cell tower) records "for the period from August 1, 2010 through October 6, 2010," the dates of the first and last of the seven robberies under investigation (DE268-1:6).

In support of its application, the government provided a detailed summary of the evidence implicating Davis in the seven robberies, including post-*Miranda* statements from two accomplices and DNA evidence found in two getaway cars (DE268-1:¶¶1-7). The magistrate judge issued the requested court order (DE266-1:1), MetroPCS disclosed the relevant records (DE283:215), and the grand jury returned a superseding indictment charging Davis with various federal offenses

(DE39).

C. Suppression Proceedings

One day before trial, Davis filed a motion to suppress the historical cell tower records produced by MetroPCS (DE272:1). Relying on *United States v. Jones*, 132 S.Ct. 945 (2012), Davis argued that "[a] basic numerical analysis of *Jones* reflects that at least five justices believe that long term location tracking by electronic means constitute[s] a Fourth Amendment search requiring a finding of probable cause and a warrant" (DE274:6). Davis did not claim that the magistrate judge violated the SCA in issuing the requested court order (DE274). Nor did he argue that the SCA is categorically unconstitutional insofar as it authorizes the disclosure of historical cell tower records without a warrant (DE274).

At the suppression hearing, the government advanced several reasons for rejecting Davis's claim. As a threshold matter, the government argued that Davis lacked Fourth Amendment standing because he had "not admitted that he either owned [or possessed] the phone" in question, and had disassociated himself from that phone by obtaining it under a fictitious alias—i.e., "Lil Wayne," the name of "a famous rapper" (DE277:31-33). On the merits, the government distinguished *Jones*, noting that the records Davis sought to suppress were "provided to us by a private company" and not obtained by means of governmental trespass (DE277:35).

In addition, the government emphasized, historical tower records are not like the real-time GPS tracking that took place in *Jones*, and could not necessarily be used to pinpoint a phone's exact location (DE277:35). At any rate, the government argued, it had relied in good faith on the SCA (DE277:33-34,38).

In response, Davis acknowledged precedent holding that "you can't have a right to privacy in something when you give false information to obtain this kind of communication device" (DE277:42). As Davis saw it, however, such precedent could be ignored as a "pre-*Jones* thought process" (DE277:42). Addressing the government's good-faith argument, Davis candidly conceded that "[t]he statute is problematic for my argument," a point he "didn't fully understand" until earlier that day (DE277:43).

Although several of the government's arguments raised factual issues—e.g., the nature and precision of the historical cell tower records here at issue, and the absence of any affirmative acknowledgement from Davis that he owned or used the unrecovered phone registered under the alias "Lil Wayne"—Davis did not present any evidence in support of his claim, either at the suppression hearing or at trial (DE277; DE285:71-101).

At the conclusion of the suppression hearing, the district court orally denied the motion to suppress (DE277:45). The court did not articulate any particular

justification for its decision (DE277:45-46). Rather, the court noted that it was "comfortable enough with the Government's position . . . to allow the evidence to go forward" (DE277:46). That ruling, the court clarified, was really only "a conditional denial" of Davis's last-minute suppression motion based on what the court knew at that point (DE277:45). Accordingly, the court invited Davis to file a post-trial motion renewing his argument, at which time the court would ask for a written response and issue a written order (DE277:45-46). Davis never filed such a post-trial motion, and the district court never issued a written order addressing Davis's claim.

D. Trial Evidence Concerning Historical Cell Tower Records

At trial, the government introduced certain MetroPCS records corresponding to four subject telephone numbers, including one ending in 5642 ("5642 number"). MetroPCS created and maintained those records in the regular course of business (DE283:207), and they were produced in response to a court order (DE283:215). The MetroPCS account for the 5642 number was registered under the name "Lil Wayne" (DE283:216; GX49). The other three phone numbers for which records were introduced were registered under the names "Nicole Baker," "Shawn Jay" and "Dope Boi Dime" (DE283:217, 219; GX49).

The government also introduced call detail records for the subject telephone

numbers, including the 5642 number (DE283:208-19; GX35). Such records contained information about the calls made or received with those phones, including the date, time, and duration of each call, along with cell site location information, which consisted of sector and tower numbers for the times when incoming and outgoing calls began and ended (DE283:206, 225-30; GX35). The records did not include tower location information for times when the phone was turned on but not being used to make or take calls (DE283:206, 229; GX35).

Davis objected to the introduction of the call-detail records for the account corresponding to the 5642 number (GX35), all of the subscriber records (GX49), and the company's cell-tower glossary (GX36) (DE283:214, 218, 227). The district court overruled those objections.

Michael Bosillo, a custodian of records from MetroPCS, provided testimony concerning the nature of the cell site information included in the toll records (DE283:219-31). Cell sites, he explained, are "the tower[s] you see all along the side of the roads" (DE283:220). The towers are needed for a phone "to work, to get a call out or to receive a call" (DE283:220). The cell phone sends a signal to a nearby tower, which is typically but not always the closest tower to the phone (DE283:220, 222, 235-37). Thus, two people driving together in the same car might be using different cell towers at the same time (DE283:223).

A cell phone tower has a circular coverage radius (DE283:222), and the "coverage pie" for each tower is divided into either three or six parts, called sectors (DE283:222, 230). The toll records listed the tower and sector numbers corresponding to each call (DE283:230). Based on those numbers, one could use a cell tower glossary to determine the physical address, including latitude and longitude, of the tower used to route the call (DE283:226; GX36).

Bosillo was unable to specify the maximum potential distance between a cell phone user and the tower used to route that user's call in an urban environment (DE283:230). Ordinarily, a cell tower would have a coverage radius of about one to one-and-a-half miles (DE283:222). In an urban area like Miami, however, "there are many, many towers," and the coverage area would be much smaller (DE283:222, 223). Whatever the precise coverage radius, the cell site information listed in the toll records could not tell you whether the caller was right next to the tower (DE283:229). Instead, the caller could "be anywhere" in the specified sector (DE283:229).

Testimonial and physical evidence adduced at trial linked Davis to the 5642 phone number. For example, cooperating codefendant Willie Smith testified that Davis used that phone number from August to October 2010, the time period encompassing all seven of the charged robberies (DE283:100). In addition,

Smith's cell phone was introduced into evidence, and the phone's contact information listed the 5642 number under Davis's nickname, "Quat" (DE283:109; GX27). Davis did not testify at trial, and he never admitted that he owned or possessed the 5642 phone. Defense counsel objected to the introduction of Smith's telephone on the ground that the phone's contact information associated Davis's nickname with the 5642 number (DE283:91-93, 97). On cross-examination, defense counsel asked Smith questions suggesting that Smith might have known more than one "Quat" (DE283:159-161).

Mitch Jacobs, a detective serving in the Miami-Dade Police Department, analyzed the historical cell site records introduced through Bosillo (DE285:19, 20). In examining the records, Detective Jacobs looked "only" at "the days that were indicated to have a robbery," and "ignore[d] all the other days" (DE285:45). Based on those records, he created maps relating to certain calls placed or received during the time periods surrounding six of the seven robberies of which Davis stood accused (DE285:23-25). The maps were introduced into evidence and published to the jury (DE285:26-38; GX37A-37F). As Detective Jacobs explained, the maps showed that, at the relevant times, phones linked to Davis and his codefendants made and received numerous calls routed via the cell towers closest to the places robbed (DE285:27-38).

On cross-examination, counsel for Davis emphasized that Detective Jacobs' maps reflected the government's representation to Detective Jacobs that the phone number in question belonged to Davis (DE285:44). Those maps, defense counsel noted, would have indicated that the phone belonged to "Mickey Mouse" if Detective Jacobs had been "told to do that" by the prosecutor (DE285:44).

3. Standards of Review

This Court reviews *de novo* the legal question whether a statute is constitutional. *United States v. Campbell*, 743 F.3d 802, 805 (11th Cir. 2014). In the context of an appeal from the denial of a suppression motion, all facts are construed in the light most favorable to the party prevailing below—here, the government. *United States v. Gibson*, 708 F.3d 1256, 1274 (11th Cir. 2013).

Summary of the Argument

I. On the facts of this case, the government did not violate Davis's Fourth Amendment rights by acquiring historical cell site records from a telephone service provider pursuant to a court order authorized by the SCA. Under the Supreme Court's third-party doctrine, MetroPCS's production of its own records to the government did not constitute a search. And, even if it did, any such search was not unreasonable within the meaning of the Fourth Amendment.

A. In order to establish a Fourth Amendment search in these circumstances,

Davis had to show two things: first, that he exhibited, by his conduct, an actual expectation of privacy in MetroPCS's business records; and second, that any such expectation was objectively reasonable. He did not make either showing.

No evidence supports the conclusion that Davis manifested an actual expectation of privacy in the records MetroPCS made to document the use of its own cell towers. Davis may not satisfy his burden of proof by adverting to statements made by the prosecutor in closing argument. Those statements were not evidence. Nor do they help his cause. It is one thing to say that Davis probably did not know his phone company was lawfully making and keeping certain routing-related records of transactions to which it was a party; it is another thing to say that he actually expected that such records could not be disclosed to others.

Even if Davis did harbor a subjective expectation of privacy in MetroPCS's records, any such expectation was not objectively reasonable. The routing-related records Davis sought to suppress were created and maintained by MetroPCS during the ordinary course of business. Under the Supreme Court's third-party doctrine, an individual has no claim under the Fourth Amendment to resist the production of business records held by a third party. *See, e.g.*, *Smith v. Maryland*, 442 U.S. 735, 99 S.Ct. 2577 (1979); *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619 (1976).

Davis may not make out a right to be secure in someone else's "papers," *see*

U.S. Const. amend. IV, by complaining that those papers contained "his location data." Evidence lawfully in the possession of a third party is not *his*, even if it has to do with *him*. Indeed, so far as the Fourth Amendment is concerned, Davis could not have prevented MetroPCS from producing the records in question even if they were his.

Davis's arguments for disregarding the Supreme Court's third-party doctrine lack merit. It is factually dubious and legally irrelevant to posit that most phone users do not know that their phone companies make and keep location-related records. As *Smith* makes clear, the public should not be presumed ignorant of undisputed and readily ascertainable facts concerning the technologies that phone companies use to provide service; such ignorance at any rate is not objectively reasonable; and an unsupported presumption of pervasive and persistent ignorance does not supply a stable or satisfactory foundation for the formulation of Fourth Amendment rights.

United States v. Jones, 132 S.Ct. 945 (2012), does not take this case outside the ambit of the third-party rule. The police in *Jones* did not obtain location information from a third party, and the Court's holding leaves the third-party doctrine untouched. Indeed, only one member of the Court even suggested that the Supreme Court should "reconsider" its third-party rule, and she did not say or imply

that the courts of appeals are not bound by that rule in the interim.

The thoughtful normative arguments advanced by Davis and his amici warrant careful consideration; but they should be directed to Congress and the state legislatures, which are in a better position to make the kinds of nuanced policy distinctions—for example, between "short-term" and "long-term" data collection, or between cell tower records and other kinds of records revealing location-related information—on which Davis's constitutional challenge is predicated.

B. Assuming Davis's Fourth Amendment rights were implicated by the application of the SCA to the facts of this case, those rights were not violated by MetroPCS's production to the government of its own records pursuant to a court order authorized by Congress. The Fourth Amendment prohibits unreasonable searches, not warrantless searches; and a "strong presumption of constitutionality is due to an Act of Congress," particularly when its validity turns on whether a search is reasonable under the Fourth Amendment. For two reasons, any "search" arguably arising out of MetroPCS's disclosure of its own records was constitutionally reasonable.

First, the SCA goes above and beyond the constitutional prerequisites governing the issuance of compulsory process. A 2703(d) order operates as a judicial subpoena, and subpoenas are not subject to the warrant procedure. Thus,

the SCA does not *lower* the bar from a warrant to a 2703(d) order; it *raises* the bar from an ordinary subpoena to one that incorporates a broad range of additional privacy protections.

Second, a traditional Fourth Amendment analysis independently supports the reasonableness of any search that took place here. Davis had, at most, a diminished expectation of privacy in business records made, kept, and owned by MetroPCS; any invasion of his privacy was minimal, particularly in light of the government's compliance with the privacy-protecting provisions of the SCA; and the challenged court order served compelling governmental interests.

II. Assuming *arguendo* that the SCA is unconstitutional as applied to this case, this Court should not hold that 2703(d) orders for historical cell tower records always violate the Fourth Amendment. Davis did not raise such a claim in the district court, and for good reason: Such a claim is at war with the very authority on which his as-applied claim is principally based. In *Jones*, the Court approved prior precedent holding that the government may monitor the whereabouts of suspects travelling in public areas with the aid of electronic devices *surreptitiously* installed in items those suspects obtained from third parties—even if such surveillance is conducted without statutory authority or judicial supervision. Reasonably construed, that settled law compels the conclusion that the government may obtain a

single point of historical cell site data to find out if a phone was in the vicinity of a public crime scene, particularly when such data is obtained from a third party pursuant to a court order authorized by Congress in a privacy-protecting statute.

Argument

I. On The Facts of This Case, The Government's Acquisition, Pursuant to an Order Authorized by The Stored Communications Act, 18 U.S.C. § 2703 (c)(1)(B), (d), of Cellular Telephone Records Showing Historical Cell Site Location Information from a Telephone Service Provider Did Not Constitute an Unreasonable Search or Seizure in Violation of Davis's Constitutional Rights Under The Fourth Amendment.[2]

In order to prevail on his as-applied claim, Davis must show two things: first, that the application of the SCA to the facts of this case involved a Fourth

[2] The government's brief addresses both of Davis's claims (and both of the issues noted in this Court's memorandum to counsel dated October 7, 2014), but it turns to his as-applied claim first. As the Supreme Court has cautioned, "[t]he constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." *Sibron v. New York*, 392 U.S. 40, 59-60, 88 S.Ct. 1889, 1901 (1968). Consistent with the general preference for as-applied adjudication of constitutional challenges, *see Gonzales v. Carhart*, 550 U.S. 124, 168, 127 S.Ct. 1610, 1639 (2007); *United States v. Raines*, 362 U.S. 17, 20-22, 80 S.Ct. 519 (1960), Davis raised only an as-applied claim in the district court and his briefing to the panel. Considering an as-applied claim first is particularly prudent where, as here, such a claim has been properly preserved and provides a sufficient basis for disposing of the case at hand. *See AFSCME v. Scott*, 717 F.3d 851, 864 (11th Cir. 2013). Finally, even if this Court deems it appropriate to decide whether the SCA always violates the Fourth Amendment insofar as it authorizes the government to acquire historical cell site records pursuant to a non-warrant court order, it may be helpful first to consider the constitutionality of the statute in a particular factual context, as established by the record developed in the proceeding below.

Amendment "search" of which he has standing to complain (i.e., that his own Fourth Amendment rights were *implicated* by the challenged governmental conduct); and second, that any such search was unreasonable within the meaning of the Fourth Amendment (i.e., that his Fourth Amendment rights were *violated* by the challenged governmental conduct). Davis fails to make either showing.

A. The application of the SCA to the facts of this case did not involve a Fourth Amendment search.

Davis's as-applied challenge to the validity of the SCA fails at the threshold because he does not meet his burden of establishing that his own Fourth Amendment rights were implicated by the contested 2703(d) order. A party may establish a Fourth Amendment search in one of two ways: first, by showing that the government engaged in conduct that "would have constituted a 'search' within the original meaning of the Fourth Amendment," *United States v. Jones*, 132 S.Ct. 945, 950 n.3 (2012); and second, by establishing that the challenged governmental conduct impinged on a reasonable expectation of privacy, *see Smith v. Maryland*, 442 U.S. 735, 739-40, 99 S.Ct. 2577, 2579-80 (1979) (citing *Katz v. United States*, 389 U.S. 347, 88 S.Ct. 507 (1967)).

Davis invokes only the latter theory. Thus, in order to show a Fourth Amendment "search" of which he has standing to complain, Davis must satisfy both

prongs of the so-called *Katz* test. The first prong asks "whether the individual has, by his conduct, 'exhibited an actual (subjective) expectation of privacy.'" *Id.* at 740, 99 S.Ct. at 2580. "The second question is whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable." *Id.* (quotation marks omitted). The following discussion considers each question in turn.

1. Davis did not meet his burden of establishing a subjective expectation of privacy in MetroPCS's business records.

In general, courts have held that phone customers could not have maintained an actual expectation of privacy in routing-related business records made by a phone company to document transactions to which it was a party. *See Smith*, 442 U.S. at 741-43, 99 S.Ct. at 2580-82; *United States v. Gallo*, 123 F.2d 229, 231 (2d Cir. 1941). There is no cause to take a different view as to cell tower records. *See In re Application of the United States*, ("*Fifth Circuit Application*"), 724 F.3d 600, 613 (5th Cir. 2013); *United States v. Madison*, 2012 WL 3095357, at *8 (S.D.Fla. 2012).

No record evidence tends to show that Davis, by his conduct, exhibited an actual expectation of privacy in MetroPCS's cell tower records. If anything, the fact that Davis (like his accomplices) registered his phone under a fictitious alias (DE283:216, 217, 219) "undercuts any claim that [he] has a subjective privacy

interest in the cell phone and thus the historical cell site information" for that phone, *United States v. Suarez-Blanca*, 2008 WL 4200156, at *7 (N.D.Ga. 2008), because it tends to evince his understanding that such information is being revealed to a third party and may be used to incriminate him. *See Madison, supra*, at *8 (noting that "the use of prepaid cell phones under false names in order to avoid law-enforcement detection . . . further demonstrates the common knowledge that communications companies regularly collect and maintain all types of non-content information regarding cell-phone communications, including cell-site tower data"); *see also United States v. Rigmaiden*, 2013 WL 1932800, at *8 (D.Az. 2013) (citing authorities and concluding that "Defendant cannot now credibly argue that he had a legitimate expectation of privacy in the devices . . . he acquired through the fraudulent use of" other people's identities).

Davis may not be excused from his burden of proof just because the prosecutor in closing argument said that Davis and his accomplices "probably had no idea that by bringing their cell phones with them to these robberies, they were allowing [their service provider] and now all of you to follow their movements on the days" of the robberies (DE287:14). The "statements and arguments of counsel are not evidence." *United States v. Lopez*, 590 F.3d 1238, 1256 (11th Cir. 2009). And, even if they were, the prosecutor's statements here do not help Davis's cause.

It is one thing to say that Davis may not have known his phone company was lawfully making and keeping certain routing-related records of transactions to which it was a party; it is another thing to say that he actually expected, much less reasonably expected, that such records could not be disclosed to others.

2. Even if Davis exhibited a subjective expectation of privacy in MetroPCS's business records, any such expectation was not objectively reasonable.

The Fourth Amendment protects "[t]he right of the people to be secure in *their* . . . papers," not in the papers of *others*. *See* U.S. Const. amend. IV (emphasis added). Consistent with the constitutional text, "an individual has no claim under the fourth amendment to resist the production of business records held by a third party." *In re Grand Jury Proceeding*, 842 F.2d 1229, 1234 (11th Cir. 1998) (citing *United States v. Miller*, 425 U.S. 435, 96 S.Ct. 1619 (1976)). That commonsense principle has long been the law, and it is fatal to Davis's claim.

In *Miller*, for example, the Court rejected a Fourth Amendment challenge to a third-party subpoena for the defendant's bank records. 425 U.S. at 440-45, 96 S.Ct. at 1622-25. As the Court explained, the bank's records were "not respondent's 'private papers,'" but "business records of the banks," in which Miller could "assert neither ownership nor possession." *Id.* at 440, 96 S.Ct. at 1623. And Miller could hardly have been surprised that the bank made and kept such records, since they

"pertain[ed] to transactions to which the bank was itself a party." *Id.* at 441, 96 S.Ct. at 1623 (quotation marks omitted). In short, Miller's Fourth Amendment rights were not even "implicated," much less violated, by "the issuance of a subpoena to a third party to obtain the records of that party." *Id.* at 444, 96 S.Ct. at 1624.

The teaching of *Miller* applies to different kinds of business records, including phone company records. *See Smith*, 442 U.S. at 741-46, 99 S.Ct. at 2580-83. In *Smith*, a telephone company installed a pen register at the request of the police to record numbers dialed from the defendant's telephone. *Id.* at 737, 99 S.Ct. at 2578. The Court expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial," since "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company" in order for their calls to be completed. *Id.* at 742, 99 S.Ct. at 2581. In any event, the Court reasoned, any such expectation was not legitimate. *Id.* at 744, 99 S.Ct. at 2582. Smith "exposed" the numbers he voluntarily dialed to the phone company, and he thereby "assumed the risk that the company would reveal to police the numbers he dialed." *Id.*

The logic of those cases applies here. Like the bank customer in *Miller* and the phone customer in *Smith*, Davis can assert neither ownership nor possession of

the third-party records he sought to suppress. Instead, those records were generated by MetroPCS, stored on its own premises, and subject to its control (DE283:206-07). Cell tower records are not the private papers of the subscriber; indeed, customers "do not generally have access to those records." *United States v. Graham*, 846 F.Supp.2d 384, 398 (D.Md. 2012). And here, as in *Smith* and *Miller*, the records pertain to transactions to which the company was a party: The records document MetroPCS's use of its own cell towers, and those towers had to be used for Davis's phone "to work"—i.e., "to get a call out or to receive a call" (DE283:220). In short, historical "cell site information is clearly a business record," and the disclosure of such information "should be analyzed under that line of Supreme Court precedent." *Fifth Circuit Application*, 724 F.3d at 611, 615.

Davis may not make out a right to be secure in someone else's "papers," *see* U.S. Const. amend. IV, by asserting that those papers contained "his location data," *see* Davis:27. Evidence lawfully in the possession of a third party is not *his*, even if it has to do with *him*. Indeed, the Fourth Amendment would not shield Davis from incriminating information in the records MetroPCS turned over even if those records were his. *See, e.g.*, *Couch v. United States*, 409 U.S. 322, 324, 335-36, 93 S.Ct. 611, 614, 619 (1973) (holding that petitioner could not reasonably claim a Fourth Amendment expectation of privacy in records in which she "retained title" after she

had "surrendered possession of the records" to her accountant).

At any rate, Davis is not in a good position to complain that the government improperly obtained "his location data," since he himself exposed and revealed to MetroPCS the very information he now seeks to keep private—i.e., the general vicinity information circumstantially inferable from cell tower records. *See Fifth Circuit Application*, 724 F.3d at 613-14; *Madison*, *supra*, at *9. "[T]he 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." *Miller*, 425 U.S. at 443, 96 S.Ct. at 1624 (emphasis added); *compare Tracey v. State*, 2014 WL 5285929, at *16 (Fla. 2014) ("Simply because the cell phone user knows or should know that his cell phone gives off signals that enable the service provider to detect its location for call routing purposes . . . does not mean that the user is consenting to use of that location information by third parties *for any other unrelated purposes*.") (emphasis added).

It is not persuasive to argue that phone users do not knowingly or intentionally disclose any location-related information to their service providers. *See* Davis:32; ACLU:20; *In re Application of the United States* ("*Third Circuit Application*"), 620 F.3d 304, 317-18 (3d Cir. 2010). In *Smith*, the Court presumed that phone users

knew of uncontroverted and publicly available facts about technologies and practices that the phone company used to make calls, document charges, and assist in legitimate law-enforcement investigations. *See* 442 U.S. at 742-43, 99 S.Ct. at 2581. Cell towers and related records are used for all three of those purposes, and *Smith*'s methodology should not be set aside just because tower records may also be used to obtain general vicinity information. Indeed, the toll records for the stationary telephones at issue in *Smith* "encompassed 'location' data with far more precision than the historical cell site location records" at issue here, and "typically that location would be one in which the user had a Fourth Amendment privacy interest, such as a home or office." *Graham*, 846 F.Supp.2d at 399.

More importantly, Davis's asserted lack of awareness that MetroPCS was lawfully documenting the use of its own cell towers does not give rise to an objectively reasonable expectation of privacy in records that the company made, kept, and owned. *See Smith*, 442 U.S. at 737, 745, 99 S.Ct. at 2578, 2582-83 (concluding that Smith's expectation of privacy was not "legitimate" even though phone companies "usually [did] not record local calls," and did so in that case only "at police request"). Ignorance of undisputed and readily ascertainable facts is both ephemeral and undeserving of constitutional protection. *See In re Application*, 809 F.Supp.2d 113, 121 (E.D.N.Y. 2011) (concluding that any "expectation of privacy in

cell-site-location records, if one exists, must be anchored in something more permanent" than the "doubtful proposition" that cell-phone users are currently "unaware of the capacities of cellular technology," since "[p]ublic ignorance as to the existence of cell-site-location records . . . cannot long be maintained").

For purposes of the Fourth Amendment, it makes no difference whether Davis knew that MetroPCS was collecting location-related information. *See United States v. Jacobsen*, 466 U.S. 109, 122, 104 S.Ct. 1652 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, *however well justified*, that certain facts will not come to the attention of the authorities.") (emphasis added). Nor does it matter whether he "consented" to their disclosure. *See* Davis:40; *Tracey*, *supra*, at *16. Like the security surveillance tapes introduced into evidence at his trial, the cell-tower records produced by MetroPCS were not his to withhold. *See Donaldson v. United States*, 400 U.S. 517, 522-23, 91 S.Ct. 534, 538 (1971); *see also id.* at 537, 91 S.Ct. at 545 (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others.").

At any rate, Davis's argument to the contrary fails on its own terms. It is undisputed that Davis's phone could not work unless it communicated with—and thereby revealed its proximity to—nearby cell towers (DE283:220); and Davis does

not deny that he wanted his phone to work.[3] Thus, Davis's main argument for disregarding the Supreme Court's third-party doctrine boils down to the claim that he intended for his phone to work, but did not intend for his phone to do what was necessary in order to work. Such an internally contradictory mindset does not and cannot form the basis for an objectively reasonable expectation of privacy. *See Smith*, 442 U.S. at 743, 99 S.Ct. at 2582 (emphasizing fact that petitioner "*had to* convey that number to the telephone company . . . if he wished to complete his call") (emphasis added); *Fifth Circuit Application*, 724 F.3d at 613 ("A cell service subscriber, like a telephone user, understands that his cell phone *must* send a signal to a nearby cell tower in order to wirelessly connect his call.") (emphasis added).

Technological advances do not give Davis a Fourth Amendment right to conceal information that otherwise would not have been private. *See United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012). The only location information contained in the records Davis sought to suppress had to do with the cell towers used to route incoming and outgoing calls (DE283:228, 229). Prior to the advent of modern switching technology and mobile telephones, those calls would have been routed by telephone operators personally connecting specified numbers assigned to

[3] As proffered at the suppression hearing, for example, two of appellant's accomplices stated that the robbers brought their cell phones to all the robberies "just in case anything went wrong and they got separated and they needed to call somebody to pick them up" (DE277:19-20).

stationary telephones. *Smith*, 442 U.S. at 744, 99 S.Ct. at 2582. A phone user who "had placed his calls through an operator . . . could claim no legitimate expectation of privacy" in routing-related information exposed to that operator, and "a different constitutional result" is not required just "because the telephone company has decided to automate." *Id.* at 744-45, 99 S.Ct. at 2582.

In certain respects, Davis has an even less viable claim than the defendants in *Miller* and *Smith*. For example, the Court in *Miller* held that a customer did not have a reasonable expectation of privacy in certain records made and kept by his bank, even though the bank was required by law to maintain those records. *See Miller*, 425 U.S. at 436, 441, 96 S.Ct. at 1621, 1623. In contrast, "[f]ederal law does not mandate that cellular providers create or maintain [historical cell tower] data," *Graham*, 846 F.Supp.2d at 398 & n.11 (citing 47 C.F.R. 42.6), and companies opt to do so only for limited periods of time (*see* ACLU:5 n.9) and legitimate business reasons, such as "to monitor or optimize service" on their networks or "to accurately bill [their] customers" for services rendered. *Fifth Circuit Application*, 724 F.3d at 611-12; *Madison*, *supra*, at *8. Hence, Davis's claim is "substantially weaker" than the claim the Court rejected in *Miller*. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 744 n.11, 104 S.Ct. 2720, 2726 n.11 (1984).

In addition, service contracts and privacy policies typically warn cell-phone

customers that phone companies collect location-related information and may disclose such data to law-enforcement authorities. *See Fifth Circuit Application*, 724 F.3d at 613. For example, MetroPCS's current privacy policy, which is accessible from the company's website, advises its wireless customers that the company "may disclose, without your consent, the approximate location of a wireless device to a governmental entity or law enforcement authority when we are served with lawful process."[4] Similarly, the company warns that its "systems capture details about the . . . location of wireless device(s) that you have"; that it "use[s] location information to route wireless communications and to provide 911 service, which allows emergency services to locate your general location"; and that it "allow[s] third parties the capability of accessing data about your location that is derived from our network." *See supra* note 4; *see also Smith*, 442 U.S. at 742-43,

[4] *See* https://www.metropcs.com/content/metro/en/mobile/metro/terms-conditions/termsconditionsdetails.privacy.html (last visited December 17, 2014). The service contract and privacy policy governing Davis's phone are not part of the record in this case. In the proceeding below, however, Davis never asserted that he did not know MetroPCS made, kept, and reserved the right to disclose records containing location-related information (DE274; DE277; DE283; DE285). Accordingly, the particular terms and conditions of his own service contract were not in dispute at the hearing convened to address his last-minute suppression motion. In addition, Davis had the burden of proving that he had a reasonable expectation of privacy in the records he sought to suppress, *Rawlings v. Kentucky*, 448 U.S. 98, 104-05, 100 S.Ct. 2556, 2561 (1980), so any doubts concerning the particular terms and conditions of his own service contract do not supply a basis for disturbing the judgment below. At a minimum, this Court should not adopt a general warrant requirement for cell tower records, without taking service contracts and privacy policies into account.

99 S.Ct. at 2581 (considering publicly available information included in phone books and other sources in assessing whether Smith had an expectation of privacy in pen-register records).

In sum, Davis asserts a constitutionally cognizable privacy interest in business records that he did not make or own and has never seen or kept; and he advances that argument even though he himself exposed to a third party the very same information he now seeks to keep private. That claim fails on its own terms, and it cannot be reconciled with the principles enunciated in *Smith* and *Miller*.

3. *Jones* does not alter the controlling analytical framework for assessing third-party disclosures.

In *United States v. Jones*, 132 S.Ct. 945 (2012), the police surreptitiously installed a GPS device on a suspect's car, and they then used that device to monitor the suspect's movements for law-enforcement purposes over a period of 28 days. *Id.* at 948. Such surveillance was not conducted pursuant to a valid court order, and it was neither authorized nor regulated by statute. *See id.* at 956 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring in the judgment). Relying on a trespass theory, the Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'" 132 S.Ct. at 949.

The holding of *Jones* has no application here, since this case does not involve any "physical intrusion" into a constitutionally protected area. *See id*. And the Court's decision leaves the third-party doctrine untouched. The police in *Jones* did not obtain any location information from a third party, so the opinion of the Court did not even "address the third-party disclosure doctrine," let alone "desert or limit it." *United States v. Wheelock*, __ F.3d __, 2014 WL 6477413, at *2 (8th Cir. Nov. 20, 2014). Only one of the nine justices even suggested that the Supreme Court should "reconsider" its third-party doctrine, and she did not say or imply that the courts of appeals are not bound by that doctrine in the interim. *See* 132 S.Ct. at 957 (Sotomayor, J., concurring).

Davis's attempt to construct an "alternative" majority from the *Jones* concurrences is unavailing. *See* Davis:43. Five justices did say that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." 132 S.Ct. at 964 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment); *id*. at 955 (Sotomayor, J., concurring) (agreeing with that statement). But a different, and partially overlapping, group of five justices took issue with that statement. *Id*. at 954. In their view, the line proposed by the principal concurrence would give rise to "thorny" and "vexing" practical problems, since there are no judicially manageable standards for

distinguishing between "short-term" and "long-term" monitoring (or, for that matter, between "most cases" and other cases that might be subject to a different standard). *See id.* at 953-54. The latter view, unlike the former, was set forth in "*the opinion of the Court*," *id.* at 948 (emphasis added).

In short, the statement on which Davis's constitutional claim is predicated cannot reasonably be construed as the past holding of an "alternative" majority; and, particularly in light of the reservations lodged by the actual majority, it is not bound to be the law in the future.

Even if it were, such law would pose no problem for the government's position here. The concurring opinions on which Davis relies do not support the proposition that the government engages in a Fourth Amendment search whenever it obtains long-term "location information," no matter what form that information takes and regardless of how and why such information is gathered. Under the SCA, law-enforcement authorities do not and may not seek historical cell tower records to spy on citizens or to keep track of their comings and goings. Instead, they consult such records to help resolve questions of historical fact "relevant and material to an ongoing criminal investigation," § 2703(d)—in this case, for example, whether Davis was or was not in the vicinities of six armed robberies at the times in question. For purposes of that inquiry, the phone company stands in the same shoes as any

other witness lawfully in possession of evidence relevant to an ongoing criminal investigation. The judicial system does not engage in "surveillance" or "monitoring" when it compels the production of preexisting documentary evidence from such a witness, *see* Fed. R. Crim. P. 17, any more than it does when a grand jury subpoenas a third-party business's security surveillance videos to find out if a particular suspect was at the scene of a crime.

By conceptualizing the problem posed by governmental "monitoring" at such a high level of generality, Davis drains the *Jones* concurrences of almost all of the facts that give them life. For example, the concurring justices in *Jones* found it troubling that "[t]he Government usurped [the defendant's] property for the purpose of conducting surveillance on him." 132 S.Ct. at 954 (Sotomayor, J.). Here, MetroPCS lawfully documented the use of its own property for legitimate business purposes. In *Jones*, the government used a surveillance method that "proceeds surreptitiously." *Id.* at 956 (Sotomayor, J.). Phone companies like MetroPCS make cell tower records openly, in accordance with applicable service contracts and privacy policies. *See Fifth Circuit Application*, 724 F.3d at 613; *supra* note 4. Most importantly, the concurring justices in *Jones* were reluctant to approve "unrestrained power" and "unfettered discretion" on the part of the police, which would empower "the Executive" to unilaterally collect sensitive information "more

or less at will" and "in the absence of any oversight from a coordinate branch." 132 U.S. at 956 (Sotomayor, J.). Here, the production of business records maintained at the discretion of a third party is congressionally authorized, subject to statutory safeguards, and judicially supervised throughout.

As the *Jones* concurrences emphasized, technology "can change" expectations of privacy, and "people may find the tradeoff" between privacy and security or convenience "worthwhile." *Id.* at 962 (Alito, J.). The national legislature is surely in a good position to periodically assess those changing expectations, and to balance them against competing interests in light of contemporary circumstances. *See Graham*, 846 F.Supp.2d at 405. Accordingly, four of the five concurring justices in *Jones* went out of their way to encourage legislative policy solutions to privacy-related problems posed by new technologies:

> 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.

132 S.Ct. at 964 (Alito, J., concurring in the judgment). The SCA embodies just such a solution. *See Fifth Circuit Application*, 724 F.3d at 614.

4. Normative arguments concerning the impact of modern technologies warrant consideration, but should be directed to Congress and the state legislatures.

As the foregoing discussion makes clear, it is not helpful to lump together doctrinally unrelated cases that happen to involve the use of "modern technology." *See, e.g.*, Davis:54-55; ACLU:22. For example, although phone companies make cell tower records with the aid of "technology," this case is otherwise nothing like *Kyllo v. United States*, 533 U.S. 27, 121 S.Ct. 2038 (2001). There, the Court held that the government engaged in a Fourth Amendment search when (1) law-enforcement officers, (2) invaded "the sanctity of the home," (3) by using a "police technology" that was "not in general public use," and (4) thereby gained information "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'" (5) absent any statutory authorization or regulation, and (6) without affording a neutral and detached magistrate a prior opportunity to assess the legality of the intrusion. 533 U.S. at 33-34, 37, 121 S.Ct. at 2043, 2045. In this case, a private party not subject to the Fourth Amendment, *see United States v. Steiger*, 318 F.3d 1039, 1045 (11th Cir. 2003), employed technologies in common use among citizens and commercial service providers to make records documenting the use of its own property; some of those records contained evidence that Davis's phone was near six public robberies;

and those records were disclosed pursuant to a court order authorized by Congress in a privacy-protecting statute.

Similarly, in *Riley v. California*, 134 S.Ct. 2473 (2014), the Court held that the police may not search the digital contents of a cell phone seized from an arrestee pursuant to the search-incident-to-arrest exception. *Id.* at 2485. But the Court there addressed a conceded "search" of information found by the police on an arrestee's phone, *id.* at 2492-93, not business records obtained from a third party in response to judicial process issued in accordance with a federal statute.

In contrast to *Kyllo* and *Riley*, the only tool the government used in this case is older than the Constitution itself. *See* XVII Oxford English Dictionary 50 (2d ed. 1989) ("He woll not come withoute he have a suppena.") (quoting letter written in 1467). In 1768, for example, William Blackstone wrote that "[i]n the hands of third persons they [*sc.* books and papers belonging to the parties] can generally be obtained by rule of court, or by adding a clause of requisition to the writ of *subpoena*, which is then called a *subpoena duces tecum*." *Id.* (quoting 1768 edition of the *Commentaries*; emphases and bracketed note in OED).

As the text of the Constitution confirms, the right of compulsory process is indispensable to the fair and effective administration of criminal justice. *See* U.S. Const. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . .

to have compulsory process for obtaining witnesses in his favor."). That is no less true—and the rights of the innocent are no less implicated—when the government rather than the accused seeks evidence relevant to an ongoing criminal investigation. *See United States v. Nixon*, 418 U.S. 683, 709, 94 S.Ct. 3090, 3108 (1974).

In light of the public's right "to every man's evidence," *id.*, the application of the third-party rule does not and should not turn on whether a third party procured its evidence with the aid of a new technology, an old technology, or no technology at all. *See On Lee v. United States*, 343 U.S. 747, 753-54, 72 S.Ct. 967, 972 (1952). Hence, the real constitutional question posed by this case is not whether the government will be allowed to "exploit evolving technologies to '*erode* the privacy guaranteed by the Fourth Amendment,'" ACLU:22 (emphasis added), but whether one—and only one—kind of business record made by private actors with the aid of technology will be constitutionally *exempt* from "congressional and judicial power" to compel the production of relevant documentary evidence. *See Oklahoma Press v. Walling*, 327 U.S. 186, 196, 66 S.Ct. 494, 499 (1946); *see also Nixon*, 418 U.S. at 706, 94 S.Ct. at 3106. Nothing in *Kyllo* or *Riley* suggests an affirmative answer to that question.

So far as the Fourth Amendment is concerned, cell tower records are not "qualitatively different" than other kinds of business records, including credit card

statements, security surveillance videos, electronic toll booth records, medical records, ATM records, and pen register records. *See* Davis:15 (quoting *Riley*, 134 S.Ct. at 2490). Indeed, many of those other records provide more precise location information than the general vicinity information circumstantially discernible from cell tower records. *See Graham*, 846 F.Supp.2d at 399. And, unlike cell tower records, other kinds of business records may be more readily used to obtain specific information about a customer's dealings with others.

The very examples offered by Davis and his amici illustrate that point. Thus, historical cell tower records may show that a particular phone was in the vicinity of an abortion clinic; but a bank or credit card statement can show that the account holder paid an abortion clinic for services rendered.[5] Tower records may show that a phone was making calls far from the user's home late at night; but hotel registry records can show that a man checked into a hotel late at night with a woman not his wife.[6] Cell site data may show that a phone was in the same part of town as the office of an unpopular political group; but pen register data can show that the phone

[5] *See Miller*, 425 U.S. at 440-43, 96 S.Ct. at 1622-24 (bank records); *Fifth Circuit Application*, 724 F.3d at 614 n.13 (credit card statements).

[6] *United States v. Willis*, 759 F.2d 1486, 1498 (11th Cir. 1985) ("hold[ing] that Willis lacks standing to challenge the officers' examination of the motel records").

made calls to and received calls from that group on a regular basis.[7] Cell tower records might prove that a phone was in the vicinity of a doctor's office; but medical records obtainable by subpoena could show that an individual actually visited that office and received specified treatment in connection with a particular ailment.[8] Cell tower information "over time" may "be used to interpolate the path the phone user travelled" (ACLU:9); but so too can electronic toll booths (like the Florida Sun Pass or the Georgia Peach Pass systems).[9] And cell tower records may show that four different phones—all registered under fictitious aliases and used as instrumentalities of crime—were in the general vicinities of six armed robberies committed in the Southern District of Florida (DE285:27-38; GX37A-37F); but security surveillance tapes can—and at times did—depict those armed assailants holding up guns to the heads of their victims (DE281:151), threatening to kill store employees while screaming profanities (DE281:228), discharging their guns during a firefight (DE283:141-42, 182-83), emptying out cash registers (DE281:131;

[7] *See Rehberg v. Paulk*, 611 F.3d 828, 843 (11th Cir. 2010) ("Rehberg lacked a legitimate expectation of privacy in the phone and fax numbers he dialed.").

[8] *See United States v. Wilk*, 572 F.3d 1229, 1236-37 (11th Cir. 2009) ("[T]he district court correctly concluded that HIPAA authorizes the disclosure of confidential medical records for law enforcement purposes, or in the course of a judicial proceeding, in response to a court order or grand jury subpoena.").

[9] *See United States v. Troya*, 733 F.3d 1125, 1136 (11th Cir. 2013) (explaining how toll booth records, cell tower records, and pen register records helped the police to unravel a "quadruple homicide" involving the "gangland-style murder of two children").

DE283:139), stealing merchandise (DE281:10-11), robbing customers of their personal belongings at gunpoint (DE283:180), shoving an elderly woman down to the ground (DE281:174), assaulting a security guard with pepper spray (DE279:25), smashing through glass display cases with sledgehammers (DE281:10-11), and even shooting at a non-threatening dog while fleeing from the scene of a crime (DE281:156; DE283:127).

As those examples make clear, many kinds of business records "can reveal a great deal about a person." ACLU:3. And for varying reasons, consumers might understandably prefer for such records not to be disclosed to others. *See Fifth Circuit Application*, 724 F.3d at 615. But such interests, however legitimate, "must be considered in light of our historic commitment to the rule of law," including "the twofold aim [of criminal justice] . . . that guilt shall not escape or innocence suffer." *Nixon*, 418 U.S. at 708-09, 94 S.Ct. at 3108. Both of those aims are implicated when a court compels the production of third-party evidence "relevant and material to an ongoing criminal investigation," § 2703(d).

The societal interest in vindicating the rights of the innocent and bringing the guilty to justice need not trump competing privacy concerns implicated by governmental access to third-party business records. Thus far, however, the principal recourse for such concerns has been "in the market or the political process:

in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections." *Fifth Circuit Application*, 724 F.3d at 615. There is no reason to believe that such solutions cannot be applied to records generated by the use of cell phones. Indeed, Congress and the state legislatures are in a particularly good position to make the kinds of nuanced policy distinctions—for example, between "long-term" and "short-term" cell tower data, between the different kinds of location-related information discernible from different kinds of business records, and between "location information" and other kinds of transaction-related information discernible from third-party records—on which Davis's constitutional challenge is predicated.

The legislature has been sensitive to such privacy concerns in the past. After *Miller*, for example, Congress enacted the Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, tit. XI, 92 Stat. 3697 et seq., in order "to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity." H.R. Rep. No. 1383, 95th Cong., 2d Sess. 33 (1978). The House Report explained that the Act was meant to supplement the Fourth Amendment, noting that "while the Supreme Court found no constitutional right of privacy in financial records, it is clear that Congress may provide protection of individual rights beyond that afforded in the Constitution."

Id. at 34. Similarly, after the Court held in *Smith* that the use of a pen register was not a Fourth Amendment search, Congress imposed limits on the government's ability to obtain electronic communications data through the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301(a), 100 Stat. 1868.

If the legislature seeks to authorize "dragnet-type" surveillance in the future (Davis:37), there will be time enough for the courts to revisit established Fourth Amendment principles. *See United States v. Knotts*, 460 U.S. 276, 284, 103 S.Ct. 1086 (1983). But, as explained in the following part, the privacy-protecting provisions of the SCA do not present any occasion for doing so now.

B. Any search arguably arising out of the SCA's application to the particular facts of this case was constitutionally reasonable.

The determination that the Fourth Amendment applies marks the beginning point, not the end, of the constitutional analysis. *Maryland v. King*, 133 S.Ct. 1958, 1969 (2013). As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is "reasonableness." *Fernandez v. California*, 134 S.Ct. 1126, 1132 (2014). "[A] warrant is not required to establish the reasonableness of all government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either." *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653, 115 S.Ct.

2390-91 (1995).

In light of those well-settled principles, Davis and his amici are wrong to assume that this Court has no choice but to strike down the SCA insofar as it authorizes any warrantless searches. *E.g.*, ACLU:10; RCFP:5. The Fourth Amendment condemns *unreasonable* searches, not *warrantless* searches; and abundant case law holds that the text means just what it says. *See, e.g.*, *Kentucky v. King*, 131 S.Ct. 1849, 1858 (2011) ("[W]arrantless searches are allowed when the circumstances make it reasonable, within the meaning of the Fourth Amendment, to dispense with the warrant requirement."). In addition, there is a "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, 96 S.Ct. 820, 824 (1976) (quotation marks omitted). That "strong presumption" has long formed part of the law of this Circuit, *see Kelly v. United States*, 197 F.2d 162, 164 (5th Cir. 1952), and it should weigh at least as heavily as the general default rule in favor of warrants.

Applying those principles here, any governmental search arguably arising out of MetroPCS's production of its own records was constitutionally reasonable, for two distinct and independent reasons.

1. The application of the SCA to the facts of this case comports with established Fourth Amendment rules governing the issuance of compulsory process.

Law-enforcement authorities did not obtain the cell tower records here at issue by storming Davis's house or raiding MetroPCS's premises. Instead, a federal prosecutor applied for a court order authorized by statute (DE268-1). The court concluded that the statutory standard was satisfied, and its order was then served on the company's custodian of records (DE266-1; DE283:205). MetroPCS chose to comply with the court's order (DE283:215). But that need not be the case. The SCA authorizes a third-party recipient to file a motion to quash, 18 U.S.C. § 2703(d), in which case further judicial proceedings must be had. Thus, a law-enforcement officer armed with a 2703(d) order may not forcibly search or seize any records, even if the recipient improperly resists production.

As that background suggests, a 2703(d) order operates as a judicial subpoena directing a third-party to produce evidence in its possession, not as a warrant authorizing a law-enforcement officer to engage in a search or seizure.[10] *Compare*

[10] Because warrants and subpoenas serve different functions and may be effectuated in different ways, there is nothing "ambiguous and contradictory," Davis:13, about the alternative statutory mechanisms for obtaining cell tower records. In some circumstances—for example, where a phone company is under investigation for fraudulent billing practices—law-enforcement authorities may deem it expedient to obtain such records by conducting a physically disruptive search of the company's files pursuant to a warrant, instead of asking the company to produce relevant

Fed. R. Crim. P. 17, *with* Fed. R. Crim. P. 41. The plain text of the statute confirms that function: An order issued under § 2703(d) directs the recipient to produce specified information; the recipient may then move to quash; and its enforcement is subject to the supervision of the issuing court. *See* 18 U.S.C. § 2703(d).

In light of their different functions, warrants and subpoenas are governed by different standards of constitutional reasonableness. *See Miller*, 425 U.S. at 446, 96 S.Ct. at 1625 (reaffirming the "traditional distinction between a search warrant and a subpoena"); *see generally In re Supboena Duces Tecum*, 228 F.3d 341, 346-49 (4th Cir. 2000) (citing authorities). "A warrant is a judicial authorization to a law enforcement officer to search or seize persons or things." *Id.* at 348. "To preserve advantage of speed and surprise, the order is issued without prior notice and is executed, often by force, with an unannounced and unanticipated physical intrusion." *Id.* Thus, "the immediacy and intrusiveness of a search and seizure conducted pursuant to a warrant demand the safeguard of demonstrating probable cause to a neutral judicial officer before the warrant issues." *Id.*

"A subpoena, on the other hand, commences an adversary process during which the person served with the subpoena may challenge it in court before

---

records pursuant to a 2703(d) order. *Cf. Zurcher v. Stanford Daily*, 436 U.S. 547, 98 S.Ct. 1970 (1978). In addition, the alternative warrant procedure may be invoked by state authorities where state law provides that such records may be obtained only with a warrant. *See* 18 U.S.C. §§ 2703(d), 2711(4).

complying with its demands." *Id.*; *see Brock v. Emerson Elec. Co.*, 834 F.2d 994, 997 (11th Cir. 1987). Hence, a subpoena need not be supported by the same showing of probable cause "literally applicable in the case of a warrant." *Oklahoma Press*, 327 U.S. at 209, 66 S.Ct. at 506. As explained in *Miller*:

> "[T]he Fourth Amendment, if applicable to subpoenas for the production of business records and papers, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant."

425 U.S. at 445-46, 96 S.Ct. at 1625 (quotation marks omitted). In keeping with the constitutional text, "[t]he gist of the protection is in the requirement, expressed in terms, that *the disclosure sought shall not be unreasonable.*" *Oklahoma Press*, 327 U.S. at 208, 66 S.Ct. at 505 (emphasis added). That has long been the law. *See Wilson v. United States*, 221 U.S. 361, 376, 31 S.Ct. 538 (1911); *Hale v. Henkel*, 201 U.S. 43, 76, 26 S.Ct. 370 (1906).

As a practical matter, it would make little sense to hold that an investigative subpoena compelling a third party's production of relevant documentary evidence may issue only upon a showing of probable cause, since often "the very purpose of requesting the information is to ascertain whether probable cause exists." *United States v. R. Enterprises*, 498 U.S. 292, 297, 111 S.Ct. 722, 726 (1991). Indeed,

"[u]nless such subpoenas are valid, it is impossible to see how the statutes can be enforced at all, or how any wrongdoer can be brought to book." *McMann v. SEC*, 87 F.2d 377, 379 (2d Cir. 1937) (Hand, J.).

In enacting the SCA, Congress protected individual privacy by requiring the government to go above and beyond the traditional constitutional prerequisites for obtaining third-party business records via the issuance of compulsory process. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1212-13 (2004). Five of the SCA's privacy-protecting provisions warrant particular mention.

First, Congress placed a neutral and detached magistrate between law-enforcement officers and the records they seek. 18 U.S.C. § 2703(d). And while a party served with a subpoena may ordinarily invoke the judicial process to resist production, Congress made the approval of a neutral and detached magistrate a precondition for the issuance of a 2703(d) order. *See id.*

Second, the SCA provides that the requested records will be made available only if a judicial officer finds "specific and articulable facts showing that there are reasonable grounds to believe" the records sought are "relevant and material to an ongoing criminal investigation." *Id.*

Third, the SCA bars "improper disclosure" of records obtained under

§ 2703(d). *See id.* § 2707(g).

Fourth, the statute provides a range of remedies and penalties for violations of the Act's privacy-protecting provisions, including money damages and the mandatory commencement of disciplinary proceedings against offending officers. *See* §§ 2707(a), (c), (d), 2712(a), (c).

Fifth, the SCA generally prohibits phone companies from voluntarily disclosing such records to "a governmental entity." *Id.* § 2702(a)(3), (c)(4), (c)(6). As that prohibition underscores, a phone company like MetroPCS would, absent privacy-protecting laws like the SCA, be free to disclose its historical cell tower records to governmental and non-governmental entities alike—without any judicial supervision, without having to satisfy the statutory standard in § 2703(d), and without even implicating the Fourth Amendment.

These statutory safeguards are not undermined by the fact that the SCA omits some of the protections tied to the warrant procedure, such as the probable-cause standard and the requirement that facts be attested under oath. The SCA does not *lower* the bar from a warrant to a 2703(d) order; it *raises* the bar from an ordinary subpoena to one with all sorts of additional privacy protections built in—at both the front and back ends. *See, e.g.*, *United States v. Guerrero*, 768 F.3d 351, 358-61 (5th Cir. 2014) (explaining that the government violated the SCA by obtaining historical

cell tower records with an ordinary subpoena, but holding that there was no Fourth Amendment violation). And Davis's complaints concerning the SCA's departures from the warrant procedure ring particularly hollow in light of the warrant-like protection afforded by the statute. After all, "[t]he primary reason for the warrant requirement is to interpose a 'neutral and detached magistrate' between the citizen and 'the officer engaged in the often competitive enterprise of ferreting out crime,'" *United States v. Karo*, 468 U.S. 705, 717, 104 S.Ct. 3302, 3304 (1984), and the SCA does just that.

In sum, the 2703(d) order here at issue comports with applicable Fourth Amendment principles. Hence, that order was constitutionally reasonable, even if Davis had "the requisite Fourth Amendment interest to challenge the validity of" the order. *See Miller*, 425 U.S. at 446, 96 S.Ct. at 1626.

2. Assuming the constitutional balance has not already been struck, a traditional Fourth Amendment analysis independently supports the reasonableness of the challenged 2703(d) order.

Absent precise guidance from the founding era, the validity of a search or seizure should be evaluated "under traditional standards of reasonableness by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of

legitimate governmental interests." *Wyoming v. Houghton*, 526 U.S. 295, 300, 119 S.Ct. 1297 (1999).

i. At most, Davis had only a diminished expectation of privacy in the third-party business records he sought to suppress.

As explained above, Davis has *no* legitimate expectation of privacy in business records made, kept, and owned by a third-party service provider. *See supra* Part I(A)(2). For the same reasons, Davis may at most assert only a *diminished* expectation of privacy in MetroPCS's records. *See King*, 133 S.Ct. at 1969 (identifying "diminished expectations of privacy" as one of the factors that "may render a warrantless search or seizure reasonable") (quotation marks and citation omitted).

ii. Particularly in light of the safeguards incorporated into the SCA, any invasion of Davis's privacy was minimal.

"[W]hether something less than probable cause may justify a search depends in part on the intrusiveness of that search." *United States v. Michael*, 645 F.2d 252, 256 n.8 (5th Cir. 1981) (en banc); *accord King*, 133 S.Ct. at 1969. Any invasion of Davis's privacy arising out of MetroPCS's production of its own records was minimal, for three reasons.

First, the way in which the government obtained those records—by serving

judicial process on a third party—involved no invasion of Davis's privacy. In this respect, 2703(d) orders are less intrusive than other kinds of warrantless searches deemed to be constitutionally reasonable. *Compare*, *e.g.*, *King*, 133 S.Ct. at 1969, 1979; *Terry*, 392 U.S. at 17 & n.13, 24-25; *Michael*, 645 F.2d at 256.

Second, the cell tower location information contained in those records was not highly private. The records here at issue could reveal that a phone was within the "general vicinity" of a particular cell tower, but they did not show whether the caller was right next to that tower (DE283:228, 229). *See Graham*, 846 F.Supp.2d at 392. Indeed, two people could be driving in the same car and using different towers, and those towers could be one-and-a-half miles apart (DE283:222, 223). And, because the records show only tower locations for the beginning and end of a call (DE:283:206, 229), they would not reflect any movements if the phone user turned off the phone, did not make or receive calls, or made one long phone call during a roundtrip journey—even if the customer traveled a considerable distance with the phone during a particular time period.

In addition, the vicinity information discernible from those records is useful only if one already has a point of reference—in this case, for example, the robbery locations—and the records themselves do not provide a basis for ascertaining that point of reference (GX35). At a minimum, the record before this Court does not

support Davis's contention that highly personal information may readily be extracted from the particular cell tower records at issue in this as-applied challenge.

Third, and most importantly, the SCA's privacy-protecting provisions guard against the improper acquisition or use of any personal information theoretically discoverable from such records. *See King*, 133 S.Ct. at 1979. In particular, the main practical concern articulated by Davis and his amici is that such records conceivably might be used—today or in the future—to draw inferences concerning private aspects of a customer's life. Under § 2703(d), however, investigative authorities may not request such customer records to satisfy prurient or otherwise insubstantial governmental interests; instead, a neutral and detached magistrate must find, based on "specific and articulable facts," that there are "reasonable grounds to believe" that the requested records are "relevant and material to an ongoing criminal investigation." Such protections are sufficient to satisfy "the primary purpose of the Fourth Amendment," which is "to prevent arbitrary invasions of privacy." *Brock*, 834 F.2d at 996; *see, e.g.*, *Terry*, 392 U.S. at 21 n.18, 88 S.Ct. at 1880 n.18 (explaining that the "demand for specificity in the information upon which police action is predicated is the central teaching of this Court's Fourth Amendment jurisprudence").

It is possible that rogue law-enforcement officers may obtain such records for

legitimate reasons, but then seek to mine them for personal information unrelated to an ongoing criminal investigation. But that same risk is present even if such records are disclosed—as Davis concedes is permissible—pursuant to a warrant based on probable cause. Moreover, Davis has offered no evidence of any kind—documentary, testimonial, or anecdotal—indicating that such abuses have ever actually happened; and still less has he shown that such abuses take place with sufficient regularity to justify constitutional invalidation of an important investigative tool authorized by Congress. *See Michael*, 645 F.2d at 258 (discounting "abstract and theoretical" invasions of privacy in assessing the reasonableness of a warrantless search) (quotation marks omitted).

In this very case, for example, the trial evidence tended to show that the government looked "only" at "the days that were indicated to have a robbery," and "ignore[d] all the other days" (DE285:45). *See King*, 133 S.Ct. at 1979 (emphasizing legitimate governmental purpose served by obtaining and testing an arrestee's DNA, and noting that "even if non-coding alleles could provide some [private medical] information, they are not in fact tested for that end"). And, even assuming that the government actually obtained any additional valuable information, such information has not been—and may not be—improperly disclosed. *See* 18 U.S.C. § 2707(g); *King*, 133 S.Ct. at 1980 ("This Court has noted

often that a statutory or regulatory duty to avoid unwarranted disclosures generally allays . . . privacy concerns.") (quotation marks omitted).

In sum, the procedure by which the government acquired the records at issue in this case involved no invasion of Davis's privacy. It does not appear that such records may readily be used to obtain any substantial quantum of private information about Davis's life; and, even if they could, the privacy-protecting provisions of the SCA amply accommodate any diminished expectation of privacy Davis may assert in MetoPCS's business records.

iii. Historical cell tower records serve important governmental interests.

Historical cell tower records are routinely used to investigate the full gamut of state and federal crimes, including child abductions, bombings, kidnappings, murders, robberies, sex offenses, and terrorism-related offenses. *See, e.g.*, *United States v. Troya*, 733 F.3d 1125, 1136 (11th Cir. 2013) ("quadruple homicide" involving the "gangland-style murder of two children"); *United States v. Mondestin*, 535 F. App'x 819 (11th Cir. 2013) (armed robbery); *United States v. Sanders*, 708 F.3d 976, 982-83 (7th Cir. 2013) (kidnapping). Such evidence is often particularly valuable during the early stages of an investigation, when the police lack probable cause and are confronted with multiple suspects. In such cases, 2703(d)

orders—like other forms of compulsory process not subject to the warrant procedure—help to build probable cause against the guilty, deflect suspicion from the innocent, aid in the search for truth, and judiciously allocate scarce investigative resources.

The societal interest in promptly apprehending criminals and preventing them from committing future offenses is "compelling." *See United States v. Salerno*, 481 U.S. 739, 750-751, 107 S.Ct. 2095, 2103 (1987). And so too is the interest in vindicating the rights of the innocent. *See King*, 133 S.Ct. at 1974. Both interests are implicated when the government seeks to compel the production of evidence relevant and material to an ongoing criminal investigation.

In sum, a traditional balancing of interests supports the reasonableness of the 2703(d) order at issue here. Davis had at most a diminished expectation of privacy in business records made, kept, and owned by MetroPCS; MetroPCS's act of producing those records did not entail a serious invasion of any such privacy interest, particularly in light of the government's compliance with the privacy-protecting provisions of the SCA; the disclosure of such records pursuant to a court order authorized by Congress served substantial governmental interests; and, given the "strong presumption of constitutionality" applicable here, residual doubts concerning the reasonableness of any arguable "search" should be resolved in favor

of the SCA.

C. The good-faith exception applies.

The exclusionary rule does not apply to evidence obtained by law-enforcement officers who acted in objectively reasonable reliance on a subsequently invalidated statute. *Illinois v. Krull*, 480 U.S. 340, 349-55, 107 S.Ct. 1160, 1167-70 (1987). As confirmed by the abundance of judicial authority upholding the constitutionality of the SCA, *see, e.g.*, *Fifth Circuit Application*, 724 F.3d at 615; *Madison*, *supra*, at *9; *Graham*, 846 F.Supp.2d at 404, it was not unreasonable for the government to rely on the 2703(d) order here at issue. *See id.* at 405. That is particularly so because the order was issued by a neutral and detached magistrate *before* the Supreme Court handed down the decision that serves as the principal legal basis for Davis's constitutional challenge (DE274). *See United States v. Leon*, 468 U.S. 897, 104 S.Ct. 3405 (1984); *United States v. Smith*, 741 F.3d 1211, 1214 (11th Cir. 2013) (discussing circuit law pre-*Jones*).

For the first time in his en banc brief, Davis now seeks to argue that the SCA may not have authorized the court order here at issue. Davis:47-52. Even if they had been properly preserved, his assorted arguments lack merit. Consistent with the plain text of the SCA, it is "well-established" that a court's statutory authority to issue a 2703(d) order "applies to historical cell site location data." *Graham*, 846

F.Supp.2d at 396 (citing authorities); *see also Third Circuit Application*, 620 F.3d at 315 ("[T]he legislative history does not show that Congress intended to exclude CSLI or other location information from § 2703(d)."). And the scrivener's error of which Davis now complains (Davis:2, 44) assuredly did not constitute a fatal "defect" in the challenged order. *See* Fed. R. Crim. P. 52(a).

Finally, the magistrate judge did not err—and still less did she reversibly err—in finding that the cell tower records for the two-month time period spanning the seven robberies were "relevant and material to an ongoing criminal investigation" (DE266-1). Cell tower data for times in between the robberies could have been used to show that the phone in question was not regularly near the site of any particular robbery, which would tend to refute claims that Davis just happened to live or work in that area. Similarly, tower data spanning the period of the charged conspiracy (and not just the discrete points in time when the particular substantive offenses were committed) could have helped to confirm that the phone registered under the alias "Lil Wayne" in fact belonged to Davis, by placing the phone user in the vicinity of various events to which Davis could be tied.

II. The Stored Communications Act, 18 U.S.C. § 2703(c)(1)(B), (d), Is Not Unconstitutional Under The Fourth Amendment Insofar as It Authorizes The Government to Acquire Records Showing Historical Cell Site Location Information from a Telephone Service Provider.

"As a general matter, courts strongly disfavor facial challenges." *AFSCME v. Scott*, 717 F.3d 851, 864 (11th Cir. 2013). The proponent of such a challenge "'must establish that no set of circumstances exists under which the Act would be valid.'" *Id.* at 863 (quoting *United States v. Salerno*, 481 U.S. 739, 745, 107 S.Ct. 2095 (1987)). Even if this Court deems it appropriate to consider the categorical challenge Davis now seeks to raise for the first time, any such claim fails under the *Salerno* standard.[11]

For the reasons set forth above, Davis's as-applied challenge to the SCA fails. Thus, this very case provides an example of a "set of circumstances" "under which the Act would be valid." *See id.* Assuming *arguendo* that Davis's as-applied claim has merit, however, "Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional." *Fifth Circuit Application*,

[11] Davis's categorical challenge is properly characterized as "quasi-facial" in nature, since he now claims that 2703(d) orders are always unconstitutional insofar as they authorize the disclosure of cell tower records, but not necessarily unconstitutional insofar as they compel the production of other kinds of phone-company records. *See AFSCME*, 717 F.3d at 863 (explaining that the *Salerno* standard applies to a claim that is "quasi-facial in nature")

724 F.3d at 615 (emphasis in original); *accord Third Circuit Application*, 620 F.3d at 313, 319 ("hold[ing] that CSLI from cell phone calls is obtainable under a § 2703(d) order and that such order does not require the traditional probable cause determination," but also determining that a court has "the option to require a warrant showing probable cause," although that option should "be used sparingly").

That conclusion follows from the very authority on which Davis primarily relies. Even before *Jones*, it was settled law that the government may monitor the whereabouts of suspects travelling in public areas with the aid of electronic devices *surreptitiously* installed in items those suspects obtained from third parties. *See Karo*, 468 U.S. at 707, 712-14, 104 S.Ct. at 3301-03; *Knotts*, 460 U.S. at 281-85, 103 S.Ct. at 1085-87. All nine members of the Court in *Jones* stood by that prior precedent, even if such covert electronic monitoring is done without prior judicial approval and in the absence of statutory authorization or regulation. *See* 132 S.Ct. at 952 ("Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location" without his knowledge); *id.* at 964 (Alito, J., concurring in the judgment) (citing *Knotts* for the proposition that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society is prepared to recognize as reasonable").

That settled law fairly compels the conclusion that the government should be able to obtain a single point of historical cell site data to help determine whether a particular phone was in the general vicinity of a public crime scene, particularly when such data is obtained from a third-party service provider pursuant to a court order authorized by Congress in a privacy-protecting statute.

It is not persuasive to argue that "even CSLI records covering a shorter period constitute a search," because "CSLI reveals or enables the government to infer information about whether the cell phone is inside a protected location" like a home. ACLU:14. Other kinds of third-party business records—including pen register records and apartment surveillance videos—enable the government to establish, and not just infer, that a person was inside a home or office at a particular time, and they do not for that cause give rise to a Fourth Amendment search. *See Graham*, 846 F.Supp.2d at 399. At any rate, it is wrong to say that a tool that *was* used only to draw inferences regarding a suspect's proximity to certain constitutionally *unprotected* places (the public sites of six armed robberies) should be struck down just because it could also have been used to draw inferences about *protected* places. By that logic, *Knotts* should have come out the other way. *See Karo*, 468 U.S. at 714, 104 S.Ct. at 3302 (distinguishing *Knotts* because "the record [in *Knotts*] did not

show that the beeper was monitored while the can containing it was inside the cabin").

Section 2703(d) orders for historical cell tower data are not more invasive than the GPS monitoring at issue in *Jones*. *See* ACLU:13. GPS monitoring is continuous, precise, and conducted in real time; historical cell tower data is sporadic, comparatively imprecise, and obtainable only for past events (DE283:228-29), the subsequent assessment of which may not be enhanced or informed by contemporaneous visual observation. While people may tend to "carry their cell *phones* with them wherever they go," ACLU:13 (emphasis added), they do not carry someone else's cell *towers* with them wherever they go; and cell site location information reveals the precise location of a cell tower, not a cell phone (DE283:220). At any rate, people also tend to take their credit cards with them wherever they go; and that does not make a subpoena for a third-party business's record of a single credit-card transaction an invalid Fourth Amendment "search," even though such a record would supply more precise location information than a single point of historical cell tower data.

The interest in formulating "categorical rules" cannot support a decision to strike down constitutionally permissible applications of the SCA. There is no Fourth Amendment overbreadth doctrine. *See United States v. Lebowitz*, 676 F.3d

1000, 1012 n.6 (11th Cir. 2012). And it is no answer to say that the distinction between "long-term" and "short-term" uses of historical cell tower data would be hard to administer. It would be. And, as the opinion of the Court in *Jones* recognized, that is good reason not to draw such an amorphous and impracticable line in the first place. *See* 132 S.Ct. at 953-54. But that concern cannot justify the decision to extend an already dubious line—if some such line must be drawn here—well beyond the scope of the only rationale that even arguably supports it.

Conclusion

The judgment of the district court should be affirmed.

Respectfully submitted,

Wifredo A. Ferrer
United States Attorney

By: /s/ *Amit Agarwal*
Amit Agarwal
Assistant United States Attorney
99 N.E. 4th Street, Suite 517
Miami, FL 33132
(305) 961-9425
Amit.Agarwal@usdoj.gov

Kathleen M. Salyer
Chief, Appellate Division

Of Counsel

Certificate of Compliance

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains **13,999** words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements for Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally-based typeface using Microsoft Word 2010, 14-point Times New Roman.

Certificate of Service

I hereby certify that twenty copies of the foregoing En Banc Brief for the United States were mailed to the Court of Appeals via Federal Express this 17th day of December, 2014, and that, on the same day, the foregoing brief was filed using CM/ECF and served via CM/ECF on all counsel of record.

/s/ *Amit Agarwal*
Amit Agarwal
Assistant United States Attorney

ab