

[PUBLISH]

IN THE UNITED STATES COURT OF APPEALS  
FOR THE ELEVENTH CIRCUIT

---

No. 12-12928

---

D.C. Docket No. 1:10-cr-20896-JAL-2

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

QUARTAVIOUS DAVIS,

Defendant-Appellant.

---

Appeal from the United States District Court  
for the Southern District of Florida

---

(May 5, 2015)

Before ED CARNES, Chief Judge, TJOFLAT, HULL, MARCUS, WILSON,  
WILLIAM PRYOR, MARTIN, JORDAN, ROSENBAUM, JULIE CARNES, and  
JILL PRYOR, Circuit Judges.

HULL, Circuit Judge:

## I. BACKGROUND

Appellant Quartavius Davis<sup>1</sup> was convicted by a jury on several counts of Hobbs Act robbery, 18 U.S.C. § 1951(b)(1), (3), conspiracy, id. § 1951(a), and knowing possession of a firearm in furtherance of a crime of violence, id. §§ 924(c)(1)(A)(ii), 2. The district court entered judgment on the verdict, sentencing Davis to consecutive terms of imprisonment totaling 1,941 months. In this appeal, we are called on to decide whether the court order authorized by the Stored Communications Act, id. § 2703(d), compelling the production of a third-party telephone company's business records containing historical cell tower location information, violated Davis's Fourth Amendment rights and was thus unconstitutional. We hold it did not and was not.

Therefore, the district court did not err in denying Davis's motion to suppress and we affirm Davis's convictions. We reinstate the panel opinion, United States v. Davis, 754 F.3d 1205 (11th Cir.), reh'g en banc granted, opinion vacated, 573 F. App'x 925 (11th Cir. 2014), with respect to all issues except those addressed in Parts I and II, 754 F.3d at 1210-18, which are now decided by the en banc court.<sup>2</sup>

---

<sup>1</sup>The Presentence Investigation Report notes that "Quartavius" is the correct spelling of appellant's first name, despite the spelling in the caption.

<sup>2</sup>Davis's advisory guidelines range was 57 to 71 months' imprisonment for his Hobbs Act robberies. However, each of his seven § 924(c) convictions required consecutive sentences. 18 U.S.C. § 924(c)(1)(D)(ii). The district court sentenced Davis to concurrent terms of 57 months'

**A. Seven Armed Robberies in a Two-Month Period**

Quartavius Davis committed seven separate armed robberies in a two-month period. From the beginning of August 2010 to the beginning of October 2010, Davis and accomplices, bearing an array of firearms, terrorized a wide range of South Florida businesses, including a pizzeria, a gas station, a drugstore, an auto parts store, a beauty salon, a fast food restaurant, and a jewelry store.

On February 18, 2011, a federal grand jury returned a seventeen-count indictment against Davis and five codefendants. Davis was named in sixteen of the seventeen counts. The indictment charged violations of the Anti-Racketeering Act, 18 U.S.C. § 1951 (Hobbs Act), and conspiracy to violate the Hobbs Act. The indictment specifically charged Davis with conspiracy to engage in Hobbs Act robbery, in violation of 18 U.S.C. § 1951(a) (Counts 1, 15); seven Hobbs Act armed robberies, in violation of 18 U.S.C. §§ 1951(a), 2 (Counts 2, 4, 6, 8, 10, 13, 16); and knowingly using, carrying, and possessing a firearm in furtherance of a crime of violence, in violation of 18 U.S.C. §§ 924(c)(1)(A)(ii), 2 (Counts 3, 5, 7, 9, 11, 14, 17).

All of Davis's codefendants pled guilty to various counts. Davis alone went to trial. The jury convicted Davis on all charged counts.

---

imprisonment on counts 1, 2, 4, 6, 8, 10, 13, 15, and 16, plus a consecutive term of 84 months on count 3, plus consecutive terms of 300 months' imprisonment on counts 5, 7, 9, 11, 14, and 17.

The panel opinion affirmed Davis's convictions but vacated the application of the guidelines sentencing increase for "brandishing" of a firearm. Davis, 754 F.3d at 1220-21, 1223. To be clear, that disposition stands.

At trial, the prosecution offered evidence of two conspiracies to commit Hobbs Act robbery and evidence that Davis took part in each conspiracy and each robbery. The prosecution further presented evidence that the conspirators committed such robberies. One member of each conspiracy testified for the government. Codefendant Willie Smith (“Smith”) testified as to the first conspiracy, encompassing six robberies at commercial establishments, including a Little Caesar’s restaurant, an Amerika Gas Station, a Walgreens drug store, an Advance Auto Parts store, a Universal Beauty Salon, and a Wendy’s restaurant. Codefendant Michael Martin (“Martin”) testified as to the second conspiracy, encompassing the robbery of a Mayors Jewelry store. Smith and Martin testified that Davis was involved in each robbery, where they wore masks, carried guns, and stole items such as cash, cigarettes, and watches.

Separately, an eyewitness, Edwin Negrón, testified regarding Davis’s conduct at the Universal Beauty Salon and the adjacent martial arts studio. He testified that Davis pointed a gun at his head, pushed both a 77-year-old woman and Negrón’s wife to the ground, and took several items from Negrón and others. Another eyewitness, Antonio Brooks, testified that Brooks confronted Davis and his accomplices outside the Wendy’s after that robbery. Brooks testified that Davis fired a gun at Brooks, and that Brooks returned fire towards the getaway car.

Beyond the accomplice and eyewitness testimony, the government produced additional evidence. Surveillance videos showed a man matching Davis's description participating in the robberies at Walgreens, Advance Auto Parts, Wendy's, and Mayors Jewelry. Smith and Martin identified Davis on the videos. DNA shown to be Davis's was recovered from the getaway car used to flee the scene of the Universal Beauty Salon robbery and the Mayors Jewelry store robbery.

In addition, the prosecution introduced telephone records obtained from MetroPCS for the 67-day period from August 1, 2010, through October 6, 2010, the time period spanning the first and last of the seven armed robberies.<sup>3</sup> The toll records show the telephone numbers for each of Davis's calls and the number of the cell tower that connected each call. A MetroPCS witness identified his company's cell tower glossary, which lists the physical addresses, including longitude and latitude, of MetroPCS's cell towers. A police witness then located on a map the precise addresses (1) of the robberies and (2) of the cell towers connecting Davis's calls around the time of six of the seven robberies. While there was some distance between them, the cell tower sites were in the general vicinity of the robbery sites.

---

<sup>3</sup>The first robbery took place on August 7, 2010, and the final robbery took place on October 1, 2010.

The location of the cell user, though, is not precise. The testimony tells us (1) the cell tower used will typically be the cell tower closest to the user, (2) the cell tower has a circular coverage radius of varying sizes, and (3) although the tower sector number indicates a general direction (North, South, etc.) of the user from the tower, the user can be anywhere in that sector. Despite this lack of precision as to where Davis's cell phone was located, the cell tower evidence did give the government a basis for arguing calls to and from Davis's cell phone were connected through cell tower locations that were near the robbery locations, and thus Davis necessarily was near the robberies too.

This appeal concerns the introduction of MetroPCS's toll records and glossary as evidence against Davis at trial. We thus review in more detail how the government acquired MetroPCS's records, the types of data in the records, and the witnesses' testimony about the records.

## **B. Court Order Regarding MetroPCS Business Records**

After Davis's arrest, the government acquired MetroPCS's business records by court order. In February 2011, the government applied to a federal magistrate judge for a court order directing various phone companies to disclose stored telephone communications records for four subject telephone numbers that included a number ending in 5642 (the "5642 number"). The application requested production of stored "telephone subscriber records" and "phone toll records,"

including the “corresponding geographic location data (cell site),” for the 5642 number. The government requested only records “for the period from August 1, 2010 through October 6, 2010.” The government sought clearly-delineated records that were both historical and tailored to the crimes under investigation.

The government did so following the explicit design of the governing statute, the Stored Communications Act (“SCA”), 18 U.S.C. § 2701 et seq. Section 2703 of the SCA provides that a federal or state governmental entity may require a telephone service provider to disclose “a record . . . pertaining to a subscriber to or a customer of such service (not including the contents of communications)” 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)(A), (B), (d). The court order under subsection (d) does not require the government to show probable cause.

No one disputes that the government’s § 2703 application to the magistrate judge contained “specific and articulable facts” showing “reasonable grounds” to believe MetroPCS’s business records—pertaining to Davis’s 5642 cell phone number—were “relevant and material” to the government’s investigation. The government’s § 2703 application provided a detailed summary of the evidence implicating Davis in the seven robberies, including post-Miranda statements from

two accomplices and the DNA evidence found in two getaway cars. Undisputedly, a sufficient showing was made to satisfy the SCA's statutory requirements.

The magistrate judge's order granted the § 2703 application. The court order required MetroPCS, the third-party cellular telephone service provider, to produce "all telephone toll records and geographic location data (cell site)" for the 5642 number during the period August 1, 2010 through October 6, 2010.

MetroPCS complied. For this two-month time period, MetroPCS produced its stored telephone records for number 5642 showing these five types of data: (1) telephone numbers of calls made by and to Davis's cell phone; (2) whether the call was outgoing or incoming; (3) the date, time, and duration of the call; (4) the number assigned to the cell tower that wirelessly connected the calls from and to Davis; and (5) the sector number associated with that tower. For ease of reference, the fourth and fifth items are collectively called "historical cell tower location information."

Importantly though, MetroPCS's business records did not show (1) the contents of any call; (2) the contents of any cell phone; (3) any data at all for text messages sent or received; or (4) any cell tower location information for when the cell phone was turned on but not being used to make or receive a call. The government did not seek, nor did it obtain, any GPS or real-time (also known as "prospective") location information.



Before trial, Davis moved to suppress MetroPCS's business records for number 5642. Although the government obtained them through a statutorily-prescribed judicial order, Davis argued the evidence should be suppressed because the § 2703(d) production of MetroPCS's records constituted a search under the Fourth Amendment and thus required probable cause and a search warrant. The district court denied the motion.<sup>4</sup>

### **C. Evidence at Trial**

During the jury trial, the government introduced the MetroPCS records for the 5642 number, which was registered to "Lil Wayne."<sup>5</sup> The government also introduced evidence tying Davis to the 5642 phone number. One of Davis's codefendants testified that Davis used the 5642 number from August 2010 to October 2010. And a codefendant's cell phone, which was entered into evidence, listed the 5642 number under Davis's nickname, "Quat," in the phone's contact list.<sup>6</sup>

---

<sup>4</sup>Davis did not present any evidence in support of his Fourth Amendment claim, either at the suppression hearing or at trial.

<sup>5</sup>MetroPCS had not required the subscriber Davis to give his true name. Instead, MetroPCS sells phones with monthly plans—averaging \$40 a month—paid up front. When that plan expires, the subscriber pays another monthly payment up front or the plan is cancelled.

<sup>6</sup>The government also obtained MetroPCS records for three other cell phone numbers used by Davis's co-conspirators, which were registered under the alias names of "Nicole Baker," "Shawn Jay," and "Dope Boi Dime." The issue before us involves only Davis's cell phone number, the 5642 number registered to "Lil Wayne." In this en banc appeal, Davis did not raise arguments about the other cell phone numbers.

Michael Bosillo, a custodian of records from MetroPCS, identified and testified about the business records regarding number 5642. He testified that MetroPCS's toll records, described above, are created and maintained in the regular course of its business.

As to cell tower location, Bosillo explained that, when a cellular phone user makes a call, the user's cell phone sends a signal to a nearby cell tower, which is typically but not always the closest tower to the phone. Two people driving together in the same car might be using different cell towers at the same time. Each cell phone tower has a circular coverage radius, and the "coverage pie" for each tower is further divided into either three or six parts, called sectors.

Bosillo testified that a cell tower would generally have a coverage radius of about one to one-and-a-half miles and that an individual cell phone user could "be anywhere" in the specified sector of a given cell tower's range. Bosillo also testified that the density of cell towers in an urban area like Miami would make the coverage of any given tower smaller, but he never said how much smaller.<sup>7</sup>

Bosillo also testified that the toll records for Davis's cell number 5642 show only (1) the number of the cell tower used to route Davis's call, and (2) the sector

---

<sup>7</sup>Davis and various amici argue that some cellular telephone companies have now increased their network coverage by augmenting their cell tower network with low-power small cells, or "femtocells," which can cover areas as small as ten meters. There is no evidence, or even any allegation, that the MetroPCS network reflected in the records in this case included anything other than traditional cell towers and the facts of this case do not require, or warrant, speculation as to the newer technology.

number associated with that tower. Thus, to determine the location of any cell tower used, Bosillo identified and explained the cell tower glossary created and kept by MetroPCS. The MetroPCS glossary listed (1) each of its cell tower numbers, (2) the physical address, including latitude and longitude, of that cell tower, and (3) how many sectors are within each cell tower's range.

This MetroPCS glossary, along with its toll records, allowed the government to determine the precise physical location of the cell towers that connected calls made by and to Davis's cell phone around the time of the robberies, but not the precise location of that cell phone or of Davis.

Davis objected to the introduction of the toll records for the account corresponding to the 5642 number, the subscriber records, and MetroPCS's cell-tower glossary. The district court overruled those objections.

The government also introduced into evidence maps that showed the locations of six of the armed robberies in relation to certain cell towers. Detective Mitch Jacobs examined the records, analyzing the records only for the days the armed robberies occurred. Detective Jacobs had, at that time, been employed by the Miami-Dade Police Department for 27 years and for the last ten years had worked with cases involving cell tower location information. He had utilized cell tower location information for his investigations of homicides, parental kidnappings, robberies, fugitives, and various other types of crime.

Detective Jacobs created the maps introduced at trial based on MetroPCS's records. These maps showed that, at or near the time of the armed robberies, cell phones linked to Davis and his codefendants made and received numerous calls routed through cell towers located in the general vicinity of the robbery locations. Detective Jacobs testified, and the maps showed, that this was true for six of the seven armed robberies. On the maps, Jacobs placed: (1) the location of the robberies and (2) the location of the cell towers that routed calls from Davis and his codefendants' phones.<sup>8</sup>

The distance between the robbery and cell tower locations was never quantified. The distance between the cell user and the cell tower was never quantified, but the evidence—records and testimony—as a whole suggests Davis's calls occurred within an area that covers at least several city blocks. The government argued the cell tower evidence showed Davis was near the robberies when they occurred.

#### **D. The Appeal**

Following his convictions by the jury, Davis appealed. A panel of this Court affirmed his convictions, but held that the government violated Davis's rights under the Fourth Amendment by obtaining stored telephone communications records from MetroPCS, a third-party telephone service provider, pursuant to the

---

<sup>8</sup>The maps did not show any cell tower's coverage radius or display any cell tower's sectors.

order of the magistrate judge issued under the SCA, 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 (11th Cir. 2014).

## II. STANDARD OF REVIEW

This Court reviews de novo constitutional challenges to a federal statute. United States v. Campbell, 743 F.3d 802, 805 (11th Cir.), cert. denied, 135 S. Ct. 704 (2014). We review the district court's legal conclusions de novo and its findings of fact for clear error. United States v. Jordan, 635 F.3d 1181, 1185 (11th Cir. 2011). 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).

## III. DISCUSSION

On appeal, Davis argues the government violated his Fourth Amendment rights by obtaining historical cell tower location information from MetroPCS's business records without a search warrant and a showing of probable cause. Davis contends that the SCA, as applied here, is unconstitutional because the Act allows the government to obtain a court order compelling MetroPCS to disclose its

historical cell tower location records without a showing of probable cause. Davis claims the Fourth Amendment precludes the government from obtaining a third-party company's business records showing historical cell tower location information, even for a single day, without a search warrant issued to that third party.

In the controversy before us, there is no GPS device, no physical trespass, and no real-time or prospective cell tower location information. This case narrowly involves only (1) government access to the existing and legitimate business records already created and maintained by a third-party telephone company and (2) historical information about which cell tower locations connected Davis's cell calls during the 67-day time frame spanning the seven armed robberies. We start by reviewing the SCA, which authorized the production of MetroPCS's business records.

#### **A. The Statute**

Under the SCA, Congress authorized the U.S. Attorney to obtain court orders requiring “a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to . . . such service (not including the contents of communications).” 18 U.S.C. § 2703(c). Section 2703 directs that a judge “shall issue” the order if the government “offers specific and articulable facts showing that there are reasonable grounds to believe that the . . .

records or other information sought[ ] are relevant and material to an ongoing criminal investigation.” Id. § 2703(d) (emphasis added). While this statutory standard is less than the probable cause standard for a search warrant, the government is still required to obtain a court order and present to a judge specific and articulable facts showing reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation. See id.

The SCA does not lower the bar from a warrant to a § 2703(d) order. Rather, requiring a court order under § 2703(d) raises the bar from an ordinary subpoena to one with additional privacy protections built in. The government routinely issues subpoenas to third parties to produce a wide variety of business records, such as credit card statements, bank statements, hotel bills, purchase orders, and billing invoices.<sup>9</sup> In enacting the SCA, Congress has required more before the government can obtain telephone records from a third-party business. The SCA goes above and beyond the constitutional requirements regarding compulsory subpoena process.

A number of the SCA’s privacy-protection provisions warrant mention. First, the SCA affords citizens protection by “interpos[ing] a ‘neutral and detached magistrate’ between the citizen and the officer engaged in the often competitive

---

<sup>9</sup>See, e.g., United States v. Willis, 759 F.2d 1486, 1498 (11th Cir. 1985) (motel registration records); United States v. Phibbs, 999 F.2d 1053, 1077 (6th Cir. 1993) (credit card statements). Those statements not only show location at the time of purchase, but also reveal intimate details of daily life, such as shopping habits, medical visits, and travel plans.

enterprise of ferreting out crime.” See United States v. Karo, 468 U.S. 705, 717, 104 S. Ct. 3296, 3304 (1984) (internal quotation marks omitted). Congress made review by a judicial officer a pre-condition for the issuance of a § 2703(d) order. Moreover, the telephone records are made available only if a judicial officer finds (or the government shows) a factual basis for why the records are material to an ongoing criminal investigation.

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

Further, the SCA bars “[i]mproper disclosure” of records obtained under § 2703(d). See id. § 2707(g). The SCA also provides remedies and penalties for violations of the Act’s privacy-protecting provisions, including money damages and the mandatory commencement of disciplinary proceedings against offending federal officers. See id. §§ 2707(a), (c), (d), 2712(a), (c).

Despite the SCA’s protections, Davis claims the court’s § 2703(d) order compelling the production of MetroPCS records violated his Fourth Amendment



rights. To prevail on his Fourth Amendment claim, Davis must show both (1) that the application of the SCA to the facts of his case involved a “search” within the meaning of the Fourth Amendment, and (2) that such search was unreasonable.

This Davis cannot do.

**B. What Constitutes a “Search”**

The Fourth Amendment guarantees “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. A party may establish a Fourth Amendment search 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, 565 U.S. \_\_\_, \_\_\_, 132 S. Ct. 945, 950 n.3 (2012). “Search” originally was tied to common-law trespass and involved some trespassory intrusion on property. See, e.g., Kyllo v. United States, 533 U.S. 27, 31-32, 121 S. Ct. 2038, 2042 (2001).

Davis makes no trespass claim, nor could he.

In 1967, the Supreme Court added a separate test—the reasonable-expectation-of-privacy test—to analyze whether a search occurred for purposes of the Fourth Amendment. 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)). The reach of the Fourth Amendment now does not turn on the presence or absence of a physical intrusion. Katz, 389 U.S. at 353, 88 S. Ct. at 512.

Thus, to determine whether the government's obtaining access to MetroPCS's records constitutes a search within the meaning of the Fourth Amendment, our lodestar is Katz's reasonable-expectation-of-privacy test. Smith, 442 U.S. at 739, 99 S. Ct. at 2579-80 (citing Katz, 389 U.S. 347, 88 S. Ct. 507).

"Katz posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search?" California v. Ciraolo, 476 U.S. 207, 211, 106 S. Ct. 1809, 1811 (1986). "Second, is society willing to recognize that expectation as reasonable?" Id. Thus, "a party alleging an unconstitutional search under the Fourth Amendment must establish both a subjective and an objective expectation of privacy to succeed." United States v. Robinson, 62 F.3d 1325, 1328 (11th Cir. 1995).

Notably, it was the interception and recording of conversations reasonably intended to be private that drove the new test and result in Katz. See 389 U.S. at 351-53, 88 S. Ct. at 511-12. The government recorded Katz's conversations by attaching an electronic listening and recording device to the outside of a public phone booth in which Katz made calls. Id. at 348, 88 S. Ct. at 509. The government had no warrant or court order of any sort. See id. at 354-56, 88 S. Ct. at 512-514. The Supreme Court held that the government's conduct in

“electronically listening to and recording the petitioner’s words violated the privacy upon which he justifiably relied while using the telephone booth,” and thus constituted a “search and seizure” under the Fourth Amendment. Id. at 353, 88 S. Ct. at 512. The critical fact was that one who enters a telephone booth, “shuts the door behind him, and pays the toll that permits him to place a call” is entitled to assume that his conversation is not being intercepted and recorded. Id. at 352, 88 S. Ct. at 511-12; id. at 361, 88 S. Ct. at 516-17 (Harlan, J., concurring).

### **C. Third Party’s Business Records**

In subsequently applying Katz’s test, the Supreme Court held—in both United States v. Miller and Smith v. Maryland—that individuals have no reasonable expectation of privacy in certain business records owned and maintained by a third-party business.

In United States v. Miller, during an investigation into tax fraud, federal agents presented subpoenas to the presidents of two banks, seeking to obtain from those banks all of Miller’s bank account records. 425 U.S. 435, 437-38, 96 S. Ct. 1619, 1621 (1976). The issue was whether the defendant Miller had a “legitimate expectation of privacy” in the documents’ contents. See id. at 440-43, 96 S. Ct. at 1622-24. The Supreme Court held that Miller had no protectable Fourth Amendment interest in the account records because the documents were: (1) business records of transactions to which the banks were parties and (2) Miller

voluntarily conveyed the information to the banks. Id. Miller had “neither ownership nor possession” over the papers and the records. Id. at 437, 440, 96 S. Ct. at 1621, 1623. Rather, the papers were “the business records of the banks.” Id. at 440-41, 96 S. Ct. at 1623. All of the bank records contained information “voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.” Id. at 442, 96 S. Ct. at 1624. The Supreme Court noted “that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” Id. at 443, 96 S. Ct. at 1624; see also In re Grand Jury Proceeding, 842 F.2d 1229, 1234 (11th Cir. 1988) (“[A]n individual has no claim under the fourth amendment to resist the production of business records held by a third party.”).

Then, in Smith v. Maryland, the Supreme Court held that telephone users have no reasonable expectations of privacy in dialed telephone numbers recorded through pen registers and contained in the third-party telephone company’s records. 442 U.S. at 742-46, 99 S. Ct. at 2581-83. The Supreme Court determined that Smith had no subjective or objective expectation of privacy in the numbers he dialed on the telephone and thus the installation of the pen register, by the

telephone company at the government's request, did not constitute a search under the Fourth Amendment. Id.

As to the subjective expectation of privacy, the Supreme Court in Smith doubted that “people in general entertain any actual expectation of privacy in the numbers they dial” because “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” Id. at 742, 99 S. Ct. at 2581. The Supreme Court stated that “[t]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.” Id. at 743, 99 S. Ct. at 2581. “Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.” Id. The Supreme Court stressed that “a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications.” Id. at 741, 99 S. Ct. at 2581.

More telling in Smith though for this case is the location information revealed through the telephone records. Smith argued that, “whatever the expectations of telephone users in general, he demonstrated an expectation of

privacy by his own conduct here, since he us[ed] the telephone in his house to the exclusion of all others.” Id. at 743, 99 S. Ct. at 2582 (internal quotation marks omitted). The Supreme Court expressly rejected Smith’s argument that he demonstrated an expectation of privacy in his own conduct here by using the telephone only in his house. The Supreme Court found that “[a]lthough [Smith’s] conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.” Id. The Supreme Court reasoned: “[r]egardless of his location, [Smith] had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.” Id.

As to the objective expectation of privacy, the Supreme Court determined that, “even if [Smith] did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not ‘one that society is prepared to recognize as reasonable.’” Id. (quoting Katz, 389 U.S. at 361, 88 S. Ct. at 516) (internal quotation marks omitted). The Supreme Court “consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” Id. at 743-44, 99 S. Ct. at 2582. The Supreme Court found that, “[w]hen he used his phone, [Smith] voluntarily

conveyed numerical information to the telephone company.” Id. at 744, 99 S. Ct. at 2582. The Supreme Court explained: “[t]he switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.” Id.

In Smith, the Supreme Court decided that “a different constitutional result is [not] required because the telephone company has decided to automate.” Id. at 744-45, 99 S. Ct. at 2582. “The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not in our view, make any constitutional difference.” Id. at 745, 99 S. Ct. at 2583. The Supreme Court concluded: “[Smith] in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and . . . even if he did, his expectation was not ‘legitimate.’” Id.

#### **D. Fifth Circuit Decision**

Before turning to Davis’s case, we review the Fifth Circuit’s recent decision holding that a court order under § 2703(d) compelling production of business records—showing this same cell tower location information—does not violate the Fourth Amendment and no search warrant is required. In re Application of the United States for Historical Cell Site Data (“In re Application (Fifth Circuit)”), 724

F.3d 600, 611-15 (5th Cir. 2013).<sup>10</sup> At the outset, the Fifth Circuit stressed who had collected the cell tower information. See id. at 609-10. The telephone company, not the government, collected the cell tower location information in the first instance and for a variety of legitimate business purposes. Id. at 611-12. The Fifth Circuit emphasized:

The Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained . . . . In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created.

Id. at 612.

The Fifth Circuit reasoned these are the telephone company's "own records of transactions to which it is a party." Id. The telephone company created the record to memorialize its business transactions with the customer. Id. at 611-12. The Fifth Circuit was careful to define business records as records of transactions

---

<sup>10</sup>The dissent mistakenly argues that we are faced with "persuasive . . . authority on both sides of the debate . . . ." Dissenting Op. at 79 n.2. To purportedly illustrate this, the dissent cites a Third Circuit decision, but that decision did not hold, as the dissent would, that a search warrant is required to obtain historical cell tower location data. In re Application of U.S. for an Order Directing a Provider of Elec. Comm'n Serv. to Disclose Records to Gov't ("In re Application (Third Circuit)"), 620 F.3d 304 (3d Cir. 2010). Rather, after the lower courts denied the government's § 2703(d) application for historical cell tower data, the government appealed and the Third Circuit actually vacated that denial. Id. at 319. The Third Circuit concluded that the SCA itself gave the magistrate judge the discretionary option to require a warrant showing probable cause and that the discretionary warrant option should "be used sparingly because Congress also included the option of a § 2703(d) order." Id.

The dissent also cites a Florida Supreme Court decision, but that case involved real-time data and did not involve a § 2703(d) order. Tracey v. State, 152 So. 3d 504, 507-08 (Fla. 2014).



to which the record-keeper business is a party. See id. It also pointed out that these business records contained no content of communications, such as the content of phone calls, letters, or emails. Id.

After discussing the nature of the business records, the Fifth Circuit, relying on Smith, explained why the cell user had no subjective expectation of privacy in such business records showing cell tower locations. The court reasoned: (1) the cell user has knowledge that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call; (2) the signal only happens when a user makes or receives a call; (3) the cell user has knowledge that when he places or receives calls, he is transmitting signals through his cell phone to the nearest cell tower and thus to his service provider; (4) the cell user thus is aware that he is conveying cell tower location information to the service provider and voluntarily does so when he uses his cell phone for calls. Id. at 613-14.

The Fifth Circuit concluded that “[c]ell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in Smith understood that the phone company recorded the numbers they dialed.” Id. at 613.<sup>11</sup> Just as the

---

<sup>11</sup>In the Fifth Circuit case, the court stated that the “contractual terms of service and providers’ privacy policies expressly state[d] that a provider uses a subscriber’s location information to route his cell phone calls” and, moreover, “that the providers not only use the information, but collect it.” In re Application (Fifth Circuit), 724 F.3d at 613. The government stresses that MetroPCS’s privacy policy, accessible from the company website, plainly states that cell tower location data may be recorded, stored, and even shared with law enforcement.

petitioner in Smith knew that when he dialed telephones, he was conveying and exposing those numbers to electronic equipment, cell phone users have knowledge they are conveying signals and exposing their locations to the nearest cell tower. Id. at 612-14.

The Fifth Circuit agreed “that technological changes can alter societal expectations of privacy,” but reasoned, “[a]t the same time, ‘[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.’” Id. at 614 (quoting United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012)). The Fifth Circuit concluded that “[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.” Id. (quoting Jones, 565 U.S. at \_\_\_, 132 S. Ct. at 964 (Alito, J., concurring)). In the end, the Fifth Circuit determined: (1) “Congress has crafted such a legislative solution in the SCA,” and (2) the SCA “conforms to existing Supreme Court Fourth Amendment precedent.” Id. The Fifth Circuit “decline[d] to create a new rule to hold that Congress’s balancing of privacy and safety is unconstitutional.” Id. at 615.

#### **E. Davis’s Case**

---

Although Davis would have signed a contract when beginning service with MetroPCS, that contract does not appear on this record to have been entered into evidence here. Thus we cannot consider it, or MetroPCS’s privacy policy, in this particular case.

Based on the SCA and governing Supreme Court precedent, we too conclude the government's obtaining a § 2703(d) court order for the production of MetroPCS's business records did not violate the Fourth Amendment.

For starters, like the bank customer in Miller and the phone customer in Smith, Davis can assert neither ownership nor possession of the third-party's business records he sought to suppress. Instead, those cell tower records were created by MetroPCS, stored on its own premises, and subject to its control. Cell tower location records do not contain private communications of the subscriber. This type of non-content evidence, lawfully created by a third-party telephone company for legitimate business purposes, does not belong to Davis, even if it concerns him. Like the security camera surveillance images introduced into evidence at his trial, MetroPCS's cell tower records were not Davis's to withhold. Those surveillance camera images show Davis's location at the precise location of the robbery, which is far more than MetroPCS's cell tower location records show.

More importantly, like the bank customer in Miller and the phone customer in Smith, Davis has no subjective or objective reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls at or near the time of six of the seven robberies.

As to the subjective expectation of privacy, we agree with the Fifth Circuit that cell users know that they must transmit signals to cell towers within range, that

the cell tower functions as the equipment that connects the calls, that users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower's range, and that cell phone companies make records of cell-tower usage. See In re Application (Fifth Circuit), 724 F.3d at 613-14. Users are aware that cell phones do not work when they are outside the range of the provider company's cell tower network. Id. at 613. Indeed, the fact that Davis registered his cell phone under a fictitious alias tends to demonstrate his understanding that such cell tower location information is collected by MetroPCS and may be used to incriminate him.

Even if Davis had a subjective expectation of privacy, his expectation of privacy, viewed objectively, is not justifiable or reasonable under the particular circumstances of this case. The unreasonableness in society's eyes dooms Davis's position under Katz. In Smith, the Supreme Court presumed that phone users knew of uncontroverted and publicly available facts about technologies and practices that the phone company used to connect 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. We find no reason to conclude that cell phone users lack facts about the functions of cell towers or about telephone providers' recording cell tower usage.

Smith's methodology should not be set aside just because cell tower records may also be used to decipher the approximate location of the user at the time of the call. Indeed, the toll records for the stationary telephones at issue in Smith included location data far more precise than the historical cell site location records here, because the phone lines at issue in Smith corresponded to stationary landlines at known physical addresses. At the time of Smith, telephone records necessarily showed exactly where the user was—his home—at the time of the call, as the user's telephone number was tied to a precise address. And the number dialed was also tied to a precise address, revealing if the user called a friend, a business, a hotel, a doctor, or a gambling parlor.

In certain respects, Davis has an even less viable claim than the defendant in Miller. For example, the Supreme Court in Miller held that a customer did not have a reasonable expectation of privacy in records made and kept by his bank even where the bank was required by law to maintain those records. See Miller, 425 U.S. at 436, 440-41, 96 S. Ct. at 1621, 1623. Here, federal law did not require that MetroPCS either create or retain these business records.

Admittedly, the landscape of technology has changed in the years since these binding decisions in Miller and Smith were issued. But their holdings did not turn on assumptions about the absence of technological change. To the contrary, the dispute in Smith, for example, arose in large degree due to the technological

advance from call connections by telephone operators to electronic switching, which enabled the electronic data collection of telephone numbers dialed from within a home. See 442 U.S. at 744-45, 99 S. Ct. at 2582-83. The advent of mobile phones introduced calls wirelessly connected through identified cell towers. This cell tower method of call connecting does not require “a different constitutional result” just “because the telephone company has decided to automate” wirelessly and to collect the location of the company’s own cell tower that connected the calls. See id. at 744-45, 99 S. Ct. at 2582. Further, MetroPCS’s cell tower location information was not continuous; it was generated only when Davis was making or receiving calls on his phone. The longstanding third-party doctrine plainly controls the disposition of this case.<sup>12</sup>

The use of cell phones is ubiquitous now and some citizens may want to stop telephone companies from compiling cell tower location data or from producing it to the government. Davis and amici advance thoughtful arguments for changing the underlying and prevailing law; but these proposals should be directed to Congress and the state legislatures rather than to the federal courts. As aptly stated

---

<sup>12</sup>To avoid the third-party doctrine, the dissent claims that “[t]he extent of voluntariness of disclosure by a user is simply lower for cell site location data.” Dissenting Op. at 80. Not so. Cell phone users voluntarily convey cell tower location information to telephone companies in the course of making and receiving calls on their cell phones. Just as in Smith, users could not complete their calls without necessarily exposing this information to the equipment of third-party service providers. The government, therefore, did not search Davis when it acquired historical cell tower location information from MetroPCS. In order to reach its result, the dissent effectively would cast aside longstanding and binding Supreme Court precedents in favor of its own view of the Fourth Amendment.

by the Fifth Circuit, “the recourse for these desires is 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.” In re Application (Fifth Circuit), 724 F.3d at 615; See also In re Application (Third Circuit), 620 F.3d at 319 (“The considerations for and against [§ 2703(d) orders not requiring a warrant] would be for Congress to balance. A court is not the appropriate forum for such balancing, and we decline to take a step as to which Congress is silent.”).

Following controlling Supreme Court precedent most relevant to this case, we hold that the government’s obtaining a § 2703(d) court order for production of MetroPCS’s business records at issue did not constitute a search and did not violate the Fourth Amendment rights of Davis.<sup>13</sup>

#### **F. United States v. Jones**

Instead of focusing on the SCA and Smith, Davis relies on United States v. Jones, 565 U.S. \_\_\_, 132 S. Ct. 945 (2012), where the government surreptitiously

---

<sup>13</sup>Rather than legal analysis, the dissent consists mainly of myriad hypothetical fact patterns and a tabloid-type parade of horrors. As the dissenting author well knows, our “decision can hold nothing beyond the facts of [this] case.” Edwards v. Prime, Inc., 602 F.3d 1276, 1298 (11th Cir. 2010) (citing Watts v. BellSouth Telecomms., Inc., 316 F.3d 1203, 1207 (11th Cir. 2003) (“Whatever their opinions say, judicial decisions cannot make law beyond the facts of the cases in which those decisions are announced.”); United States v. Aguillard, 217 F.3d 1319, 1321 (11th Cir. 2000) (“The holdings of a prior decision can reach only as far as the facts and circumstances presented to the Court in the case which produced that decision.” (quotation marks omitted))).

attached a GPS device to a private vehicle and used its own device to track the vehicle's movements over a four-week period. Id. at \_\_\_, 132 S. Ct. at 948. In Jones, the Supreme Court held that the government's physical intrusion on the defendant's private property<sup>14</sup> was a "search" and violated the Fourth Amendment. Id. at \_\_\_, 132 S. Ct. at 949. Significantly, the government-initiated physical trespass in Jones led to constant and real-time GPS tracking of the precise location of the defendant's vehicle. Id. at \_\_\_, 132 S. Ct. at 948.<sup>15</sup> "The Government physically occupied private property for the purpose of obtaining information." Id. at \_\_\_, 132 S. Ct. at 949. The Supreme Court had "no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." Id.

The majority opinion in Jones acknowledged that "later cases, of course, have deviated from [an] exclusively property-based approach" and have adopted an alternative "reasonable expectation of privacy" standard. Id. at \_\_\_, 132 S. Ct. at 950 (citing Katz, 389 U.S. at 351, 360, 88 S. Ct. at 511, 516 (majority opinion and opinion of Harlan, J., concurring)). But the result in Jones required nothing other

---

<sup>14</sup>The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. "It is beyond dispute that a vehicle is an 'effect' as that term is used in the Amendment." Jones, 565 U.S. at \_\_\_, 132 S. Ct. at 949.

<sup>15</sup>The Supreme Court explained: "By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period." Jones, 565 U.S. at \_\_\_, 132 S. Ct. at 948.



than the property-based approach. Though the government argued Jones had no “reasonable expectation of privacy,” the Supreme Court majority determined it “need not address the Government’s contentions, because Jones’s Fourth Amendment rights d[id] not rise or fall with the Katz formulation.” Id.

Explaining the distinction, the majority opinion stressed that “the Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.” Id. at \_\_\_, 132 S. Ct. at 952. But the majority holding in Jones turned on the physical intrusion of the government placing a GPS device on a private vehicle. Id. at \_\_\_, 132 S. Ct. at 949.

That is not this case. The government’s obtaining MetroPCS records, showing historical cell tower locations, did not involve a physical intrusion on private property or a search at all. The records belonged to a private company, not Davis. The records were obtained through a court order authorized by a federal statute, not by means of governmental trespass. MetroPCS, not the government, built and controlled the electronic mechanism (the cell towers) and collected its cell tower data for legitimate business purposes. Jones is wholly inapplicable to this case.

Davis and the dissent attempt to deploy the concurrences in Jones to argue that historical cell tower location data is the equivalent of GPS and constitutes the sort of precise, long-term monitoring requiring the government to show probable

cause. This attempt misreads the concurrences. We review the concurrences in detail because they leave the third-party doctrine untouched and do not help Davis's case. If anything, the concurrences underscore why this Court remains bound by Smith and Miller.

Justice Sotomayor concurred in the majority opinion, but was concerned because the government's GPS monitoring had "generate[d] a precise, comprehensive record of a person's public movements" and gave the government "unrestrained power to assemble data." Id. at \_\_\_, 132 S. Ct. at 955-56. She found the "[r]esolution of [that] difficult question[]" was "unnecessary . . . because the Government's physical intrusion on Jones' Jeep supplie[d] a narrower basis for decision." Id. at \_\_\_, 132 S. Ct. at 957 (emphasis added). In joining the majority's opinion, she provided the fifth vote for the physical trespass holding. Id.

Justice Sotomayor did state: "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Id. (citing Smith, 442 U.S. at 742, 99 S. Ct. at 2581; Miller, 425 U.S. at 443, 96 S. Ct. at 1624). But she quickly added and countered her own suggestion, stating: "[p]erhaps, as Justice ALITO notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' post, at 962, and perhaps not."

Id. Justice Sotomayor, writing alone, raised a question, but did not even purport to answer it.

Justice Alito's concurrence further underscores why this Court is bound by Supreme Court precedent in Smith and Miller. Justice Alito concurred in the judgment and explained why the government-initiated, and government-controlled, real-time constant GPS monitoring violated the Fourth Amendment. Id. at \_\_\_, 132 S. Ct. at 957-64. Only the government did the tracking and its tracking was not authorized or regulated by a federal statute. See id. at \_\_\_, 132 S. Ct. at 956 (Sotomayor, J., concurring); id. at \_\_\_, 132 S. Ct. at 964 (Alito, J., concurring in the judgment). Justice Alito's focus is on unrestrained government power.

The context of his concurrence is critical. Nothing Justice Alito says contravenes the third-party doctrine. His concurring opinion does not question, or even cite, Smith, Miller, or the third-party doctrine in any way. The opinion never uses the words "third party" or "third-party doctrine." It would be a profound change in jurisprudence to say Justice Alito was questioning, much less casting aside, the third-party doctrine without even mentioning the doctrine.

Further, Justice Alito's concurrence speaks only at a high level of abstraction about the government's placement and control of an electronic GPS mechanism on a private vehicle that did the precise, real-time, and long-term monitoring. See id. at \_\_\_, 132 S. Ct. at 962-64. In stark contrast, the mechanism

in Davis’s case is MetroPCS’s own electronic mechanism—the cell tower. MetroPCS created and assembled the electronic data. The government obtained access only through judicial supervision and a court order. Nothing in Justice Alito’s concurrence in any way undermines the third-party doctrine. If anything, Justice Alito’s concurrence, joined by three others, suggests that a legislative solution is needed. *Id.* at \_\_\_, 132 S. Ct. at 964 (“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.” (citation omitted)). At present, the SCA is that solution.

Not only are Davis and the dissent ignoring controlling law, but even the internal logic of their arguments fails.<sup>16</sup>

First, historical cell tower location data is materially distinguishable from the precise, real-time GPS tracking in *Jones*, even setting aside the controlling third-party doctrine discussed above. Historical cell tower location data does not identify the cell phone user’s location with pinpoint precision—it identifies the cell tower that routed the user’s call. The range of a given cell tower will vary given

---

<sup>16</sup>The dissent remarks that we “ignore[ ] the opinion of five Justices of the Supreme Court at [our] own risk.” Dissenting Op. at 91, n.7. Quite the contrary, the majority opinion has faithfully recounted the two concurring opinions in *Jones* in the factual context of the case actually decided by the Supreme Court. Furthermore, because *Jones* involved a government trespass and not the third-party doctrine, eight of the nine Justices did not write or join one word about the “third-party doctrine,” much less criticize it. It is the dissent that ignores, and fails to follow, binding Supreme Court precedent.

the strength of its signal and the number of other towers in the area used by the same provider. While the location of a user may be further defined by the sector of a given cell tower which relays the cell user's signal, the user may be anywhere in that sector. This evidence still does not pinpoint the user's location. Historical cell site location data does not paint the "intimate portrait of personal, social, religious, medical, and other activities and interactions" that Davis claims.

Second, reasonable expectations of privacy under the Fourth Amendment do not turn on the quantity of non-content information MetroPCS collected in its historical cell tower location records. The § 2703(d) order covered 67 days of MetroPCS records. In his brief before this en banc Court, Davis argued that the length of the records covered by the order made the production an unconstitutional "search." But at oral argument Davis's counsel firmly contended that even one day of historical cell tower location information would require a search warrant supported by probable cause. Counsel's response at oral argument is faithful to Davis's broader claim, but misapprehends the governing law. Because Davis has no reasonable expectation of privacy in the type of non-content data collected in MetroPCS's historical cell tower records, neither one day nor 67 days of such records, produced by court order, violate the Fourth Amendment.<sup>17</sup>

---

<sup>17</sup>The SCA necessarily limits the time span of telephone records for which the government may secure a court order, as the government must show that such records are "relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

As an extension of the argument above, Davis and various amici argue that cell tower data potentially implicating the home is due particular Fourth Amendment protection. In addition to noting the Supreme Court's clear rejection of this argument as it concerned toll records in Smith, we find it useful to recount the manner in which the evidence about Davis's home tower arose in this case.

On cross-examination by Davis's trial counsel, Detective Jacobs was asked whether a person's calls made from his or her home may be connected through a single cell tower—the "home tower." Detective Jacobs responded that they may be. Defense counsel followed up, asking whether, "[o]n the other hand . . . you might see more than one tower" even though the person remains in his or her house? Again, Detective Jacobs responded yes. At that time, defense counsel was arguing the imprecision of the data collected. Like two riders in the same car, a user's calls from his home may be connected by different towers if more than one tower is located in range of the home. The government only discussed Davis's home tower after it was introduced by the defense, and only did so to illustrate that none of the robberies were committed in the vicinity of the home tower.

MetroPCS produced 67 days of historical cell site location information for Davis's cellular phone. Davis, a prolific cell phone user, made approximately 86 calls a day.<sup>18</sup> Without question, the number of calls made by Davis over the course

---

<sup>18</sup>This number comes from an analysis of Davis's cell phone usage by the American Civil

of 67 days could, when closely analyzed, reveal certain patterns with regard to his physical location in the general vicinity of his home, work, and indeed the robbery locations. But no record evidence here indicates that the cell tower data contained within these business records produces precise locations or anything close to the “intimate portrait” of Davis’s life that he now argues.<sup>19</sup> The judicial system does not engage in monitoring or a search when it compels the production of preexisting documents from a witness.

### **G. Reasonableness**

Even if this Court were to hold that obtaining MetroPCS’s historical cell tower locations for a user’s calls was a search and the Fourth Amendment applies, that would begin, rather than end, our analysis. Maryland v. King, 569 U.S. \_\_\_, \_\_\_, 133 S. Ct. 1958, 1969 (2013). The Fourth Amendment prohibits unreasonable searches, not warrantless searches. As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is

---

Liberties Union in its capacity as amicus curiae in this case. While all 67 days of toll records were placed in evidence against Davis, the government witnesses analyzed Davis’s cell phone usage only for the seven days on which the armed robberies occurred.

<sup>19</sup>Davis now also argues that the Supreme Court’s recent decision in Riley v. California, 573 U.S. \_\_\_, 134 S. Ct. 2473 (2014), where law enforcement officers seized the cell phones of arrestees and then searched the contents of the phones without obtaining warrants, supports his claim of an unconstitutional search. Riley held that this warrantless search of the contents of a cell phone obtained incident to an arrest violated the Fourth Amendment. Id. at \_\_\_, 134 S. Ct. at 2485. But the Supreme Court in Riley made a special point of stressing that the facts before it “do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.” Id. at \_\_\_, 134 S. Ct. at 2489 n.1. It is not helpful to lump together doctrinally unrelated cases that happen to involve similar modern technology.

“reasonableness.” Fernandez v. California, 571 U.S. \_\_\_, \_\_\_, 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 Sch. Dist. 47J v. Acton, 515 U.S. 646, 653, 115 S. Ct. 2386, 2390-91 (1995).

Simply put, the reasonableness of a search or seizure is 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, 1300 (1999). 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) (internal quotation marks omitted).

This traditional Fourth Amendment analysis supports the reasonableness of the § 2703(d) order in this particular case. As outlined above, Davis had no reasonable expectation of privacy in business records made, kept, and owned by MetroPCS. At most, Davis would be able to assert only a diminished expectation of privacy in MetroPCS’s records. See King, 569 U.S. at \_\_\_, 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 omitted)).

Further, any intrusion on Davis’s alleged privacy expectation, arising out of MetroPCS’s production of its own records pursuant to a § 2703(d) order, was minimal for several reasons. First, there was no overhearing or recording of any conversations. Second, there is no GPS real-time tracking of precise movements of a person or vehicle. Even in an urban area, MetroPCS’s records do not show, and the examiner cannot pinpoint, the location of the cell user. Ironically, Davis was using old technology and not the new technology of a smartphone equipped with a GPS real-time, precise tracking device itself.

Third, a § 2703(d) court order functions as a judicial subpoena, but one which incorporates additional privacy protections that keep any intrusion minimal. The SCA guards against the improper acquisition or use of any personal information theoretically discoverable from such records. See King, 569 U.S. at \_\_\_, 133 S. Ct. at 1979-80. Under § 2703(d), investigative authorities may not request such customer-related records merely 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 v. Emerson Elec. Co., Elec. & Space Div., 834 F.2d 994, 996 (11th Cir. 1987); see, e.g., Terry v. Ohio, 392 U.S. 1, 21 n.18, 88 S. Ct. 1868, 1880 n.18 (1968) (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”).

The stored telephone records produced in this case, and in many other criminal cases, serve compelling governmental interests. Historical cell tower location 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, 821 (11th Cir. 2013) (unpublished) (per curiam) (armed robbery); United States v. Sanders, 708 F.3d 976, 982-83 (7th Cir. 2013) (kidnapping). Such evidence is 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 search 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, 750-51, 107 S. Ct. 2095, 2103 (1987). But so too is the societal interest in vindicating the rights of innocent suspects. See King, 569 U.S. at \_\_\_, 133 S. Ct. at 1974. Both interests are heavily implicated when the government seeks to compel the production of evidence “relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Cell tower location records have the capacity to tell the police investigators that an individual suspect was in the general vicinity of the crime scene or far away in another city or state.

In sum, a traditional balancing of interests amply 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; the production of those records did not entail a serious invasion of any such privacy interest, particularly in light of 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, any residual doubts concerning the reasonableness of any arguable “search” should be resolved in favor of the

government. Hence, the § 2703(d) order permitting government access to MetroPCS's records comports with applicable Fourth Amendment principles and is not constitutionally unreasonable.<sup>20</sup>

#### IV. CONCLUSION

For the reasons set forth above, we affirm the judgment of conviction and vacate only that portion of the sentence attributable to the enhancement for brandishing.<sup>21</sup>

---

<sup>20</sup>In the alternative, we hold that the prosecutors and officers here acted in good faith and therefore, under the well-established Leon exception, the district court's denial of the motion to suppress did not constitute reversible error. See United States v. Leon, 468 U.S. 897, 919-21, 104 S. Ct. 3405, 3418-19 (1984).

<sup>21</sup>Because there are multiple opinions, it may be helpful to summarize the final count. Nine members of the en banc court agree there was no Fourth Amendment violation in this case. Seven members of the court join the majority opinion. Two members of the court, Judges Wilson and Jordan, join the majority opinion as to its reasonableness holding.

WILLIAM PRYOR, Circuit Judge, concurring:

I join the majority opinion in full, but I write separately to explain that a court order compelling a telephone company to disclose cell tower location information would not violate a cell phone user's rights under the Fourth Amendment even in the absence of the protections afforded by the Stored Communications Act, 18 U.S.C. §§ 2701–2712, and as judges of an inferior court, we must leave to the Supreme Court the task of developing exceptions to the rules it has required us to apply.

It is well-established that “the application of the Fourth Amendment depends on whether the person invoking its protection can claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’ that has been invaded by government action.” *Smith v. Maryland*, 442 U.S. 735, 740, 99 S. Ct. 2577, 2580 (1979) (citations omitted). And the Supreme Court has made clear that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743–44, 99 S. Ct. at 2582. There is no doubt that Davis voluntarily disclosed his location to a third party by using a cell phone to place or receive calls. For that reason, this appeal is easy.

*Smith* controls this appeal. In *Smith*, the Supreme Court held that, because telephone users voluntarily convey the phone numbers they dial to their telephone companies, the installation of a pen register at police request to record those

numbers did not constitute a “search” under the Fourth Amendment. *Id.* at 742–46, 99 S. Ct. at 2581–83. But just as telephone users voluntarily convey the phone numbers they dial to a telephone company’s switching equipment, cell phone users too voluntarily convey their approximate location to a carrier’s cell towers.

To the extent that *Smith* is distinguishable from this appeal, *Smith* presents a *closer* question, because in this appeal the government did not request that MetroPCS maintain records of its customers’ cell phone calls. MetroPCS decided what business records to maintain, and the government sought the records of Davis’s calls after the fact. And those records contained location information that Davis voluntarily conveyed to MetroPCS by placing calls that were routed through nearby cell towers, which are a familiar part of our landscape.

That Davis had no legitimate expectation of privacy in the information he conveyed to MetroPCS follows from a straightforward application of the third-party doctrine, completely aside from the additional protections of the Stored Communications Act. The Act provides that a court order for disclosure “shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[] are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Davis does not dispute that the government complied with the Act. But the greater protections afforded telephone customers

under the Act do not disturb the constitutional principle that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Smith*, 442 U.S. at 743–44, 99 S. Ct. at 2582. So Davis would have no legitimate expectation of privacy in the information he conveyed to MetroPCS even if Congress repealed the Act tomorrow. A court order compelling a carrier to disclose cell tower location information does not violate a cell phone user’s rights under the Fourth Amendment any more than a court order compelling a bank to disclose customer account information, *see United States v. Miller*, 425 U.S. 435, 96 S. Ct. 1619 (1976).

The dissent’s argument that *Smith* is distinguishable from this appeal because the disclosure of location information to cell carriers is less “voluntary” and less “knowing,” Dissenting Op. at 78-80, than the disclosure of dialed telephone numbers makes no sense. The dissent argues that the disclosure of location information is less “voluntary” than the disclosure of dialed telephone numbers because “cell phone users do not affirmatively enter their location in order to make a call,” *Id.* at 78, but in neither case is a phone user coerced to reveal anything. If a telephone caller does not want to reveal dialed numbers to the telephone company, he has another option: don’t place a call. If a cell phone user does not want to reveal his location to a cellular carrier, he also has another option: turn off the cell phone. That Davis had to disclose his location in order to place or

receive a call does not distinguish this appeal from *Smith*, because, as the dissent admits, telephone callers “have to” convey dialed numbers to the telephone company in order to place calls, Dissenting Op. at 78. That a caller “affirmatively enter[s]” phone numbers but a cell phone user does not “affirmatively enter” his location when he places or receives a call may implicate the user’s *knowledge* that he is conveying information to a third party, but it does not make the latter disclosure less *voluntary* than the former. Davis’s disclosure of his location was also no less “knowing” than the disclosure at issue in *Smith*. In *Smith*, the Supreme Court explained that “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.” 442 U.S. at 742, 99 S. Ct. at 2581. Similarly, cell phone users realize that their calls are routed through nearby cell towers. It is no state secret that cell phones work less effectively in remote areas without cell towers nearby. As the Court made clear in *Smith*, that “most people may be oblivious to” the “esoteric functions” of a technology is consistent with most people having “some awareness” of its purpose. *Id.* at 742, 99 S. Ct. at 2581. In the light of common experience, it is “too much to believe,” *id.* at 743, 99 S. Ct. at 2581, that cell phone users lack “some awareness,” *id.* at 742, 99 S. Ct. at 2581, that they communicate information about their location to cell towers.



If the rapid development of technology has any implications for our interpretation of the Fourth Amendment, it militates in favor of judicial caution, because Congress, not the judiciary, has the institutional competence to evaluate complex and evolving technologies. “Judges cannot readily understand how . . . technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical.” Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 858–59 (2004). Our decisions resolve adversarial proceedings between parties. Legislatures, by contrast, must consider “a wide range” of factors and balance the opinions and demands of competing interest groups. *Id.* at 875. “The task of generating balanced and nuanced rules requires a comprehensive understanding of technological facts. Legislatures are well-equipped to develop such understandings; courts generally are not.” *Id.* Simply put, we must apply the law and leave the task of developing new rules for rapidly changing technologies to the branch most capable of weighing the costs and benefits of doing so.

As judges of an inferior court, we have no business in anticipating future decisions of the Supreme Court. If the third-party doctrine results in an unacceptable “slippery slope,” Dissenting Op. at 85, the Supreme Court can tell us as much. *See, e.g., Hohn v. United States*, 524 U.S. 236, 252–53, 118 S. Ct. 1969,

1978 (1998) (“Our decisions remain binding precedent until we see fit to reconsider them, regardless of whether subsequent cases have raised doubts about their continuing vitality.”); *Rodriguez de Quijas v. Shearson/Am. Express, Inc.*, 490 U.S. 477, 484, 109 S. Ct. 1917, 1921–22 (1989) (“If a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls, leaving to this Court the prerogative of overruling its own decisions.”); *Evans v. Sec’y, Fla. Dep’t of Corr.*, 699 F.3d 1249, 1263 (11th Cir. 2012) (“We must not, to borrow Judge Hand’s felicitous words, ‘embrace the exhilarating opportunity of anticipating’ the overruling of a Supreme Court decision.”) (internal citation omitted). That is, if “the Supreme Court has given reasons to doubt the rule’s breadth,” Dissenting Op. at 80, it alone must decide the exceptions to its rule.

JORDAN, Circuit Judge, concurring, in which WILSON, Circuit Judge, joins:

This case is certainly about the present, but it is also potentially about the future. Although the Court limits its decision to the world (and technology) as we knew it in 2010, *see* Maj. Op. at 10 n.7 & 31 n.13, its holding that Mr. Davis lacked an expectation of privacy in service provider records used to establish his cell site location may have implications going forward, particularly given the Court's reliance on the third-party doctrine. *See, e.g., Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435, 442-43 (1976). As technology advances, location information from cellphones (and, of course, smartphones) will undoubtedly become more precise and easier to obtain, *see generally Planet of the Phones*, THE ECONOMIST (Feb. 28, 2015), and if there is no expectation of privacy here, I have some concerns about the government being able to conduct 24/7 electronic tracking (live or historical) in the years to come without an appropriate judicial order. And I do not think I am alone in this respect. *See United States v. Jones*, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring, joined by Ginsburg, Breyer, and Kagan, JJ.) (“[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”); *id.* at 955 (Sotomayor, J., concurring) (“I agree with Justice Alito that, at the very least,

‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’”).<sup>1</sup>

As a result, I would decide the Fourth Amendment question on reasonableness grounds and leave the broader expectation of privacy issues for another day, much like the Supreme Court did in *City of Ontario v. Quon*, 560 U.S. 746, 759-60 (2010) (assuming that police officer had an expectation of privacy in text messages he sent from his city-provided pager, even though those messages were routed through and kept by a third-party service provider, and resolving the case on reasonableness grounds). I would assume that Mr. Davis had a reasonable expectation of privacy—albeit a diminished one—and hold that the government satisfied the Fourth Amendment’s reasonableness requirement by using the procedures set forth in 18 U.S.C. § 2703(d) to obtain a court order for Mr. Davis’ cell site records.

## I

The Fourth Amendment’s “basic purpose . . . is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials.”

---

<sup>1</sup>Three decades ago, a defendant in a case before the Supreme Court argued that allowing the police to place a digital beeper in a container filled with chloroform, in order to monitor the container’s location, would lead to “twenty-four hour surveillance of any citizen in this country . . . without judicial knowledge or supervision.” *United States v. Knotts*, 460 U.S. 276, 283-84 (1983). The Supreme Court’s response to that assertion was that “if such dragnet type law enforcement practices as [the defendant] envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.” *Id.*

*Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967). “As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is ‘reasonableness.’” *Maryland v. King*, 133 S.Ct. 1958, 1969 (2013) (citation and internal punctuation omitted).

“The reasonableness of a search,” the Supreme Court recently explained, “depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations.” *Grady v. North Carolina*, 135 S. Ct. 1368, 1371 (2015). These circumstances include, among others, “the means adopted” by the government to effectuate the search. *See Carroll v. United States*, 267 U.S. 132, 168 (1925).

## II

At times, circumstances may render a warrantless search or seizure reasonable. One such scenario is when there are “diminished expectations of privacy.” *King*, 133 S. Ct. at 1969 (citation and internal punctuation omitted). Although I am prepared to assume that Mr. Davis enjoyed some expectation of privacy, *cf.* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 8 (2012) (defining privacy, in today’s digital world, in terms of control rather than secrecy, because practical necessities now require individuals to share information about themselves “with trusted individuals and institutions for limited purposes”), I think it is fair to say

that such an expectation was somewhat diminished, and not full-throated, due to the third-party doctrine. After all, *Smith* indicates that a person gives up control of certain information when he makes and receives calls from a phone. Although *Smith* does not fit this case like a glove—cellphones and smartphones (and the vast amounts of information they contain and can generate) are qualitatively different from land-line phones—it is nevertheless relevant that the cell site information the government obtained existed due to calls Mr. Davis made and received on his cellphone.<sup>2</sup>

On the other side of the ledger, Mr. Davis' cell site information was not obtained or seized “outside the judicial process, without prior approval by a judge or magistrate.” *Coolidge v. New Hampshire*, 403 U.S. 443, 454-55 (1971). *Cf. Johnson v. United States*, 333 U.S. 10, 13-14 (1948) (noting that the Fourth Amendment’s “protection consists in requiring that . . . inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime”). The government secured the cell site records under a provision of the Stored Communications Act. And that provision requires a magistrate judge—a neutral judicial officer—to review an

---

<sup>2</sup> I recognize that some of the cell site information resulted from calls Mr. Davis received but never answered. For obvious reasons, however, Mr. Davis did not make (and has not made) a nuanced Fourth Amendment argument differentiating between data generated from calls he made and answered and data generated from calls he merely received without answering. Such an argument would not have been of much help to Mr. Davis, who sought to suppress all of the cell site data the government obtained.

application and determine whether the government has offered “specific and articulable facts showing that there are reasonable grounds to believe that the [cell cite location information] sought [is] relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). Significantly, “there is a strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is ‘reasonable[,]’” *United States v. Watson*, 423 U.S. 411, 416 (1976) (citation and some internal punctuation omitted), and this strong presumption attaches to § 2703(d).

As explained briefly below, the government articulated the necessary “specific and articulable facts.” I therefore agree with the Court that the magistrate judge’s order, which authorized the government to obtain the cell site information, satisfied the reasonableness requirement of the Fourth Amendment. *See Camara*, 387 U.S. at 528.<sup>3</sup>

The government’s application for Mr. Davis’ cell site information stated the following: Willie Smith confessed that he and Mr. Davis were involved in the

---

<sup>3</sup> For whatever it is worth, the Supreme Court has on occasion held that the phrase “reasonable grounds,” as used in certain federal narcotics laws, is essentially the same as “probable cause” for purposes of the Fourth Amendment. *See Draper v. United States*, 358 U.S. 307, 310 n.3 (1959); *Wong-Sun v. United States*, 371 U.S. 471, 478 n.6 (1963). And it has said that “[t]he substance of all the definitions of probable cause is a reasonable ground for belief of guilt.” *Maryland v. Pringle*, 540 U.S. 366, 371 (2003) (citation and internal punctuation omitted). So maybe the evidentiary showing required by § 2703(d) is not too far removed from the probable cause normally demanded for warrants under the Fourth Amendment. *But cf. Griffin v. Wisconsin*, 483 U.S. 868, 872-77 (1987) (differentiating between “reasonable grounds” standard and “probable cause” standard).

robberies of a Little Caesar's restaurant, the Universal Beauty Salon, and a Wendy's restaurant in Miami, Florida; Jamarquis Terrell Reid admitted that he had participated with Mr. Davis in the robberies of an Amerika gas station, a Walgreens store, and an Advance Auto Parts store in Miami, Florida; Michael Martin told the authorities that he and Mr. Davis had robbed a Mayor's jewelry store in Weston, Florida; Mr. Davis' DNA was recovered from a stolen BMW that was used as the getaway car in the Mayor's jewelry store robbery; the robberies in question took place between August 7, 2010, and October 1, 2010; and Mr. Smith and Mr. Reid each said that, at the time of certain of the robberies (those of the Little Caesar's restaurant, the Amerika gas station, the Advance Auto Parts store, and the Universal Beauty Salon), Mr. Davis' cellphone number was the 5642 number. Not surprisingly, Mr. Davis conceded at oral argument that the government could have secured a warrant (had it elected to do so) for the cell site information because it had the necessary probable cause.

The temporal scope of the request, moreover, was reasonable. The government sought cell site information spanning from August 1, 2010, to October 6, 2010—a 67-day period which began six days before the first known robbery and ended six days after the last known robbery. The government explained in its application that those records would “assist law enforcement in determining the locations of [Mr. Davis] on days when robberies in which [he was] suspected to



have participated occurred,” and “whether [he] communicated with [the] other [individuals] on the days of the robberies and, if so, how many times.”

Finally, it is important to reiterate that the cell site information was generated from calls Mr. Davis made and received on his cellphone, and was not the result of his merely having his cellphone turned on. There was, in other words, no passive tracking based on Mr. Davis’ mere possession of a cellphone, and I do not read the Court’s opinion as addressing such a situation. *See* Maj. Op. at 8, 30.

### III

For me, this is one of those cases where it makes sense to say less and decide less. *See* CASS R. SUNSTEIN, ONE CASE AT A TIME 4-10 (1999); ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH 111-13 (1st ed. 1962). “Prudence counsels caution before the facts in the instant case are used to establish . . . premises that define the existence, and extent, of privacy expectations.” *Quon*, 560 U.S. at 759.

With these thoughts, I join Parts I, II, III.G, and IV of the Court’s opinion and concur in the judgment.

ROSENBAUM, Circuit Judge, concurring.

I concur in the Majority's opinion. I write separately, though, because, like the Dissent, I think that the third-party doctrine,<sup>1</sup> as it relates to modern technology, warrants additional consideration and discussion. I view the third-party doctrine as applying in this case because *Smith v. Maryland*, 442 U.S. 735, 99 S. Ct. 2577 (1979), implicitly found no historical expectation of privacy implicated by the information that we give to a service provider for the purpose of making a telephone call other than the expectation of privacy that we generally do not have in information that we voluntarily convey to a third party. Since, like *Smith*, this case involves information that we knowingly expose to a service provider for the purpose of making a telephone call and no more specific historically recognized privacy interest is implicated by cell-site location information, this case is necessarily controlled by *Smith*.

But when, historically, we have a more specific expectation of privacy in a particular type of information, the more specific privacy interest must govern the Fourth Amendment analysis, even though we have exposed the information at issue to a third party by using technology to give, receive, obtain, or otherwise use the protected information. In other words, our historical expectations of privacy do

---

<sup>1</sup> The third-party doctrine applies when a person voluntarily entrusts information to a third party, and it generally renders the Fourth Amendment's warrant requirement inapplicable as it pertains to the procurement of the exposed information from the third party. See *United States v. Miller*, 425 U.S. 435, 442-43, 96 S. Ct. 1619, 1624 (1976).

not change or somehow weaken simply because we now happen to use modern technology to engage in activities in which we have historically maintained protected privacy interests. Neither can the protections of the Fourth Amendment. *See Kyllo v. United States*, 533 U.S. 27, 34, 121 S. Ct. 2038, 2043 (2001) (“To withdraw protection of this minimum expectation [of privacy] would be to permit . . . technology to erode the privacy guaranteed by the Fourth Amendment.”). So reliance on the third-party doctrine must be limited to those cases involving alleged privacy interests that do not implicate a more specific historically recognized reasonable privacy interest.

## I.

Before exploring why this is so, I pause to express my view that the Dissent is right to raise its concerns. In our time, unless a person is willing to live “off the grid,” it is nearly impossible to avoid disclosing the most personal of information to third-party service providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling. Today’s world, with its total integration of third-party-provided technological services into everyday life, presents a steroidal version of the problems that Justices Marshall and Brennan envisioned when they dissented in *United States v. Miller*, 425 U.S. 435, 447, 454, 96 S. Ct. 1619, 1626, 1629 (1976) (Brennan, J., and Marshall, J.,

dissenting, respectively), and its progeny, including *Smith v. Maryland*, 442 U.S. 735, 748, 99 S. Ct. 2577, 2584 (1979) (Marshall, J., dissenting). As Justice Marshall aptly explained the problem, under the third-party doctrine, “unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.” *Smith*, 442 U.S. at 750, 99 S. Ct. 2577, 2585 (Marshall, J., dissenting). Perhaps it was this type of realization that caused Justice Sotomayor to write, “[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” *United States v. Jones*, \_\_\_ U.S. \_\_\_, 132 S. Ct. 945, 957 (Sotomayor, J., concurring). Since we are not the Supreme Court and the third-party doctrine continues to exist and to be good law at this time, though, we must apply the third-party doctrine where appropriate.

But, as the Dissent points out, the mere fact that the third-party doctrine could have been applied to an alleged privacy interest does not mean that it always has been. To ensure that this is a case where the third-party doctrine should be applied, I think it important to consider what sets apart those cases where the Supreme Court has chosen not to apply the third-party doctrine, despite the fact that a party has exposed its effects or information to a third party.

## II.

The Supreme Court has explained that, in analyzing a Fourth Amendment claim, we begin by determining “whether the action was regarded as an unlawful search or seizure under the common law when the Amendment was framed.” *Wyoming v. Houghton*, 526 U.S. 295, 299, 119 S. Ct. 1297, 1300 (1999). We do this because, “[a]t bottom, we must ‘assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.’”<sup>2</sup>

---

<sup>2</sup> Some might suggest that we must first determine whether a search within the meaning of the Fourth Amendment has occurred, and only if one has should we then assess whether that search has violated a constitutionally protected expectation of privacy, in the context of engaging in a reasonableness analysis. But generally, when the alleged search is of information and it is not accompanied by a concurrent physical trespass, we must evaluate whether a reasonable expectation of privacy existed in the information in the first place in order to determine whether a “search” has occurred. See *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967); *Smith*, 442 U.S. 735, 99 S. Ct. 2577. That inquiry requires us to resolve the conflict between the historical expectation of privacy allegedly violated by the search and the third-party doctrine’s rule that no expectation of privacy exists when a person voluntarily exposes information to a third party. And under the reasonableness analysis, we balance the degree to which a search or seizure “intrudes upon an individual’s privacy” against “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, 1300 (1999). So we would again need to figure out the relationship between the competing historical expectation of privacy and the third-party doctrine to determine the ultimate expectation of privacy to weigh against the government’s interest. As a result, this two-step analysis becomes redundant in the context of an alleged search of information without a concurrent physical trespass.

Moreover, if, in conducting the reasonableness analysis, we ignore the historical privacy interest and always defer to the third-party doctrine, that does not account for the way in which the Supreme Court has resolved the conflict between the historical privacy interest and the third-party doctrine in cases like *Katz*, 389 U.S. 347, 88 S. Ct. 507, because ignoring the historical privacy interest in favor of the third-party doctrine would always result in a determination that no warrant is required under a reasonableness evaluation. This is necessarily so because when the third-party doctrine applies, by definition, there is no reasonable privacy interest to weigh on the individual’s side of the scale against the government’s interest in crime fighting. But “the normal need for law enforcement” generally cannot exempt a search from the warrant requirement where the searched party enjoys a reasonable expectation of privacy, *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 653, 115 S. Ct. 2386, 2391 (1995), such as when the privacy

*United States v. Jones*, \_\_\_ U.S. \_\_\_, 132 S. Ct. 945, 950 (2012) (citation omitted).

So it seems to me that existing Supreme Court precedent may fairly be construed to suggest that where society has historically recognized a legitimate expectation of privacy, we must continue to do so for purposes of Fourth Amendment analysis, even if, in our modern world, we must now expose to a third party information that we would have previously kept private, in order to continue to participate fully in society. If we do not, we will face the Hobson's choice of leaving our historically

---

interest at stake has historically been recognized—unless, of course, it is impracticable to obtain a warrant under the circumstances. *See, e.g., Terry v. Ohio*, 392 U.S. 1, 88 S. Ct. 1868 (1967). And if we resolved the conflict between the historically existing privacy interest and the third-party doctrine by assuming a diminished expectation of privacy in the historical interest being weighed against the government's general interest in crime fighting, that still would not seem to account for cases like *Katz*, 389 U.S. 347, 88 S. Ct. 507, even if the Court found that satisfying a lesser requirement than probable cause, such as that set forth by § 2703(d), was necessary to obtain the information. Indeed, I am aware of no case where the Court has expressly found an expectation of privacy diminished because of the third-party doctrine and yet has concluded that a warrant was required. *But cf. Riley v. California*, \_\_\_ U.S. \_\_\_, 134 S. Ct. 2473, 2488 (2014) (holding that a warrant is generally required to search an arrestee's cell phone, even though arrestees have a diminished expectation of privacy because of their status as arrestees). Whether we ignored the more specific historical privacy interest in favor of the third-party doctrine or found that the historical privacy interest was diminished, though, privacy interests long recognized as reasonable by society, which therefore historically necessitated a showing of probable cause and a warrant under the Fourth Amendment in order to breach, would be violated without a warrant and on a showing of less than probable cause, simply because we happen to use technology to do more efficiently what we used to do without technology. I do not believe that Supreme Court precedent supports the conclusion that the long-established privacy interests protected by the Fourth Amendment should be subject to the whims of technology. *See Kyllo*, 533 U.S. at 34, 121 S. Ct. at 2043 (2001) (“To withdraw protection of this minimum expectation [of privacy] would be to permit . . . technology to erode the privacy guaranteed by the Fourth Amendment.”). And even if the Court were prepared to conclude that a privacy interest diminished by the third-party doctrine nonetheless required a warrant to breach, it would still need to articulate why one particular expectation of privacy diminished by the third-party doctrine was sufficient to outweigh the government's general interest in crime fighting, while a different expectation of privacy diminished by the third-party doctrine was not, unless the more specific historical expectation of privacy negates the effects of the third-party doctrine in evaluating the privacy interest for purposes of conducting the reasonableness analysis.

recognized Fourth Amendment rights at the door of the modern world or finding ourselves locked out from it. That the Constitution will not abide.

A.

As the Dissent points out, the Supreme Court has held that “[a] hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office.” *Hoffa v. United States*, 385 U.S. 293, 301, 87 S. Ct. 408, 413 (1966); *see also Minnesota v. Carter*, 525 U.S. 83, 95-96, 119 S. Ct. 469, 476 (1998) (Scalia, J., concurring) (citing *Oystead v. Shed*, 13 Mass. 520 (1816), for the proposition that a trespass occurs when the sheriff breaks into a dwelling to capture a boarder living there); *Minnesota v. Olson*, 495 U.S. 91, 96-97, 110 S. Ct. 1684, 1688 (1990) (holding that overnight guests in the homes of a third person can have a reasonable expectation of privacy in those premises). This is so, even though housekeepers and maintenance people commonly have access to hotel rooms during a guest’s stay and can view and even move around a guest’s belongings in order to conduct their duties. But the fact that a hotel guest has exposed his or her belongings to hotel workers does not, in and of itself, entitle the government to enter a rented hotel room and conduct a warrantless search.

Similarly, historically, human operators were known to eavesdrop on the contents of telephone calls in the early days of telephone usage. *See* Jeff Nilsson,

*What the Operators Overheard in 1907*, The Saturday Evening Post, June 30, 2012, <http://www.saturdayeveningpost.com/2012/06/30/history/post-perspective/operators-heard-1907.html> (last visited Apr. 16, 2015). And, as Justice Stewart observed, even after human operators were taken out of the equation, telephone conversations may have been “recorded or overheard by the use of other [telephone] company equipment.” *Smith v. Maryland*, 442 U.S. 735, 746, 99 S. Ct. 2577, 2583 (1979) (Stewart, J., dissenting). But the fact that, historically, we exposed our private conversations to third parties did not stop the Supreme Court from holding in *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507 (1967), that we have a reasonable expectation of privacy in telephone communications and that the government generally must obtain a warrant before intercepting them.

Why should that be so when the third-party doctrine also speaks to what a reasonable expectation of privacy is (none where it applies), and the doctrine seemingly applies to these situations? I believe that Supreme Court precedent fairly may be read to suggest that the third-party doctrine must be subordinate to expectations of privacy that society has historically recognized as reasonable. Indeed, our privacy expectations in modern-day hotels and the content of our telephone conversations hearken back to historically recognized reasonable expectations of privacy.



As Justice Scalia has explained, “The people’s protection against unreasonable search and seizure in their ‘houses’ was drawn from the English common-law maxim, ‘A man’s home is his castle.’” *Carter*, 525 U.S. at 95, 119 S. Ct. at 475 (Scalia, J., concurring) (emphasis omitted). And a person enjoys a recognized expectation of privacy in that home, provided he or she actually is living there. *Id.* at 95-96, 119 S. Ct. at 476. So, when a person rents and dwells in a hotel room,<sup>3</sup> that hotel room becomes that person’s “home” and “castle,” for purposes of the Fourth Amendment, regardless of who else may enter the premises.

As for the telephone, it, of course, was not invented until the late 1800’s and was not widely used until well after the Framers’ time.<sup>4</sup> Until then, people who were not closely located to each other typically communicated by letter. *See, e.g.*, <https://jeffersonpapers.princeton.edu/> (last visited Apr. 16, 2015) (noting that Thomas Jefferson wrote and received letters). As the Supreme Court has noted, “Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy . . . .” *United States v.*

---

<sup>3</sup> I recognize that inns existed in the Framers’ day.

<sup>4</sup> Alexander Graham Bell obtained a patent for the telephone on March 7, 1876. *See* <http://www.pbs.org/transistor/album1/addlbios/bellag.html> (last visited Apr. 16, 2015). He successfully transmitted speech over the line five days later. *Id.* But the United States House of Representatives has since recognized Antonio Meucci as the inventor of the telephone. H.R. Res. 269, 107th Cong. (June 11, 2002). Meucci reportedly developed the first version of a working telephone in 1860. *See id.*

*Jacobsen*, 466 U.S. 109, 114, 104 S. Ct. 1652, 1657-58 (1984); *see also Ex parte Jackson*, 96 U.S. 727, 733, 24 L. Ed. 877 (1877).

While the Supreme Court did not mention society's reasonable expectation of privacy in the content of communications sent by letter through third parties when it found a reasonable expectation of privacy in the content of communications transmitted by telephone through third parties in *Katz*, it is clear that the historical expectation of privacy in communications by letter is the same expectation of privacy that we continue to have in communications that we conduct by telephone. And the fact that we have always had to rely on third parties to engage in telephone calls—even when the third parties were known to eavesdrop from time to time—does not somehow change our reasonable expectation of privacy in personal telephone calls. Put simply, the fact that we have changed the way that we conduct personal communications does not mean that we have altered our expectation of privacy in our personal communications.

## **B.**

To help explain how the conflict between historically recognized privacy interests and the third-party doctrine plays out in light of modern technology—and why the cell-site location information at issue in this case is subject to the third-party doctrine—consider a few examples of historical privacy interests implicated by modern technology.

If our expectation of privacy in our personal communications has not changed from what it was when we only wrote letters to what it is now that we use telephones to conduct our personal interactions, it has not changed just because we now happen to use email to personally communicate.<sup>5</sup> *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010). Just as the need to entrust third parties with our personal conversations when we communicate by written letter or by telephone does not affect the analysis, the need to rely on third parties to provide Internet service when we communicate by email cannot do so, either.

The same is true for our other historically recognized reasonable expectations of privacy. So, for instance, while the Internet and its search engines obviously did not exist in the 18th century, libraries did. *See, e.g.,*

---

<sup>5</sup> The Supreme Court has held that addressing and other routing information on paper letters, like pen-register and trap-and-trace information (including the date and time of listed calls) regarding telephone calls, is accessible to the government without a warrant. *See Ex parte Jackson*, 96 U.S. 727, 736, 24 L. Ed. 877; *Smith*, 442 U.S. 735, 99 S. Ct. 2577. Email routing information, such as the sender, the receiver, the date, the time, and other routing information (such as Internet Protocol addresses) implicates the same expectations of privacy as older versions of routing information found on paper letters and in pen-register and trap-and-trace information. *See United States v. Forester*, 512 U.S. 500, 511 (9th Cir. 2007). The lack of a reasonable expectation of privacy in routing information as it pertains to paper letters and telephone conversations does not change just because the medium for engaging in personal conversations does. Subject lines in emails, however, are not in any way related to the routing or transaction information of an email; no one writes the subject matter of the letters they send on the outside of the envelope, and people do not give the telephone service provider a general overview of the telephone conversations they are about to have. So subject-matter lines on emails cannot be governed by the lack of an expectation of privacy attending paper-letter or telephone-call routing information. Instead, subject-matter lines usually disclose a summary or general statement about the content of the email communication itself, and the privacy interest implicated by subject-matter lines is therefore the same as the privacy interest in personal communications conducted by paper letters and telephone calls. As a result, as with the content of paper letters and telephone conversations, a reasonable expectation of privacy exists in the subject-matter lines of emails.

[http://franklinma.virtualltownhall.net/Pages/FranklinMA\\_Library/libraryhistory](http://franklinma.virtualltownhall.net/Pages/FranklinMA_Library/libraryhistory) (last visited Apr. 13, 2015) (discussing the establishment of the Franklin Public Library in 1790). And, though libraries no doubt have always kept track of the books checked out, they have not monitored what a person reviews within the borrowed books, and library users have traditionally been free to anonymously peruse materials at the library without checking them out and creating a record. This anonymity is critical to First Amendment rights. *See, e.g., United States v. Rumely*, 345 U.S. 41, 57-58, 73 S. Ct. 543, 551-42 (1953) (Douglas, J., concurring) (“When the light of publicity may reach any student, any teacher, inquiry will be discouraged. . . . If [a reader] can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries . . . of the land).

This privacy interest is no less important simply because many of us now use the Internet to do what we used to do at the library. We do not have lower expectations of privacy in what we research—particularly with respect to our expectations that the government will not be looking over our shoulders to review our work—merely because we research and read it online at home or in a coffee shop instead of in hard copies of books and periodicals in the stacks of the library, even though the only way that we can conduct online research is through a third-party service provider. In short, the expectation of privacy in reading and

researching what we want, free from government surveillance without a warrant, has not changed just because the mechanism we use for engaging in this conduct has evolved.

As for documents that we store in the Cloud, our privacy interest there is the same as that recognized in documents and other items maintained in a rented office or residence, or a hotel room during a paid visit. As discussed previously, the Supreme Court has plainly recognized as reasonable under the Fourth Amendment the privacy interest in effects held in such places, even though a straight-forward application of the third-party doctrine would suggest the opposite conclusion, particularly in the case of a hotel room, where housekeeping and maintenance workers can be expected to enter the premises. The privacy expectation has not abraded simply because the effect to be searched is virtual and the “place” of storage is now the intangible Cloud. *Cf. Riley v. California*, \_\_\_ U.S. \_\_\_, 134 S. Ct. 2473, 2494-95 (2014) (recognizing that searches of cell phones implicate the same type of privacy interest invaded by the “reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity,” and holding that a warrant is generally required to search a cell phone in an arrestee’s possession at the time of arrest, despite the historical rule allowing for a search of

effects on an arrestee at the time of arrest). “For the Fourth Amendment protects people, not places.” *Katz*, 389 U.S. at 351, 88 S. Ct. at 511.

C.

And Justice Alito’s concurrence in *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment), suggests a viable and apt historical privacy interest that pertains to global-positioning system information: the expectation of privacy as it regards incessant surveillance. Justice Alito has described this expectation of privacy as follows:

[R]elatively short-term monitoring of a person’s movements on public streets accords with expectations of privacy that our society has recognized as reasonable. . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.

*Id.*

Three other Justices joined in Justice Alito’s *Jones* concurrence, and another, Justice Sotomayor, expressed her agreement with the idea that, “at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’” *Id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring)). While this view may not constitute binding Supreme Court precedent, it certainly suggests that society has long

viewed as reasonable the expectation of privacy in not being subjected to constant, longer-term surveillance. And if that's the case, the only question that remains about whether the government must obtain a warrant to engage in longer-term GPS monitoring is where we draw the line establishing what constitutes "longer-term" GPS monitoring. But that is not a question that we must answer today.

Nevertheless, in my opinion, the longer-term GPS issue necessarily means that the Dissent is correct in its concerns that the expectation of privacy that is infringed by longer-term GPS monitoring may, at some point, become the same expectation of privacy implicated by more and more precise cell-site location technology. When that happens, the historical reasonable expectation of privacy in not being subjected to longer-term surveillance may well supersede the third-party doctrine's applicability to information entrusted to third parties as it pertains to cell-site location information.<sup>6</sup> But that is not this case.

According to the MetroPCS records custodian who testified in this case, the radii of the cell towers at issue were approximately a mile to a mile and a half. Since a sector is generally a one-third to a one-sixth pie slice of the roughly

---

<sup>6</sup> One other perhaps significant difference between GPS technology and precise cell-site location information also exists: GPS monitoring is constant, whereas cell-site location information is produced only when a cell-phone user makes or receives a call. If a person is usually on the cell phone, that may be a distinction without a difference. But if a person is not, that may be a meaningful dissimilarity. We conduct Fourth Amendment jurisprudence "with an eye to the generality of cases." *See Houghton*, 526 U.S. at 304, 119 S. Ct. at 1303 (balancing interests under the Fourth Amendment's reasonableness approach). So that factual issue may require resolution at a future time.

circular tower range, that means that, at best, the government was able to determine where Davis was within approximately 14,589,696 square feet.<sup>7</sup> In an urban environment, this is not precise enough to rival the invasion of privacy that pinpoint-longer-term surveillance represents.

Since no specific historical privacy interest is implicated by cell-site location information, and further, because the privacy interest in the cell-site location information at issue here is materially indistinguishable from the privacy interest in the pen-register information at stake in *Smith*,<sup>8</sup> we must apply the third-party doctrine, as the Supreme Court did in *Smith*. I read *Smith*, in turn, as implicitly finding no historical privacy interest implicated by information provided to the telephone company to allow a call to be made, other than the general third-party

---

<sup>7</sup> A one-mile radius (5,280 feet), squared (27,878,400), times  $\Pi$ , equals 87,538,176 square feet, divided by six (one sector), equals 14,589,696 square feet.

<sup>8</sup> I respect the Dissent's thought process in attempting to distinguish the concept of whether cell-phone users know that they are disclosing to their service providers the fact that they are usually located in the range of the nearest cell towers that their cell phones are using when they make and receive calls, from the Supreme Court's conclusion in *Smith* that standard telephone users know that they are disclosing the telephone numbers that they are calling when they dial. But it seems to me that the average cell-phone user knows that cell phones work only when they are within service range of a cell tower. Advertising campaigns are built on this concept. See, e.g., <https://www.youtube.com/watch?v=OPwPo-IAQ-E> (last visited Apr. 13, 2015) ("Can you hear me now?"); <https://www.youtube.com/watch?v=VZPjJI0K7Bk> (last visited Apr. 13, 2015) ("There's a map for that"). In *Smith*, similar to the Dissent here, Justice Marshall argued that the third-party doctrine did not apply, in part, because people do not "typically know" that a phone company monitors call[] [information] for internal reasons." 442 U.S. at 748-49, 99 S. Ct. at 2584-85. Right or wrong, he lost that battle. And, while cell-site location information is certainly not pen-register information and I can understand where the Dissent is coming from, I do not feel comfortable taking the position that the average cell-phone user does not know that he or she is disclosing location information to the cell-service provider.



doctrine.<sup>9</sup> Because no specific historical privacy interest is implicated by pen-register-type information, the more general historical privacy expectation associated with the third-party doctrine governed in *Smith*. The same is true with respect to the cell-site location information at issue in this case.

### III.

Nevertheless, where, as here, no historical privacy interest exists in the information sought, Congress always has the option of legislating higher standards for the government to obtain information. Justice Alito has opined, “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. *Jones*, 132 U.S. at 964 (Alito, J., concurring in the judgment). This is certainly one potential limitation on the third-party doctrine. And we have seen Congress enact legislation in response to the application of the third-party doctrine to our modern world. *See, e.g.*, the Right to Financial Privacy Act, 12 U.S.C. § 2701, *et seq.*<sup>10</sup> Indeed, the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510, *et seq.*, of which the Stored Communications Act, 18 U.S.C. §§ 2701-2712, is a part—the statute under

---

<sup>9</sup> This makes sense, as the privacy interest in discreet routing information is the same as the privacy interest in address information on letters, which, in turn, has always been subject to the third-party doctrine. *See supra* at n.5.

<sup>10</sup> *See* H.R. Rep. No. 95-1383 at 9306 (1978) (“The Title is a congressional response to the Supreme Court decision in the *United States v. Miller* . . . . The Court did not acknowledge the sensitive nature of [financial records], and instead decided that since the records are the ‘property’ of the financial institution, the customer has no constitutionally recognizable privacy interest in them.”).

which the government obtained the order authorizing it to receive Davis's historical cell-site location information in this case—was enacted (and later amended), in part, to protect what Congress recognized as “privacy interests in personal and proprietary information” that travels and is maintained in electronic form by third-party service providers. *See* H.R. Rep. No. 99-541 at § I (1986).

But legislation should fill only the gaps that occur when no historically recognized privacy interest is implicated by the technology under review. The legislature, after all, does not have the power to entirely redefine the protections of the Fourth Amendment each time that it enacts a new law. While providing more protection than the Fourth Amendment requires represents a choice that Congress may, within its power, make, providing less is not a constitutional option. If it were, the Fourth Amendment would be meaningless because it would simply be whatever Congress said it was at any given time.

That cannot be right under our Constitution. So Congress's ability to legislate reasonable expectations of privacy (other than when Congress elects to increase expectations above the Fourth Amendment baseline) must be limited to, at most, only those circumstances where no historical privacy interest implicated by the technology under review exists.

#### IV.

For all of these reasons, I believe that *Smith* (and therefore, the third-party doctrine) inescapably governs the outcome of this case. But when we must necessarily expose information to third-party technological service providers in order to make use of everyday technology, and the technological service merely allows us to engage in an activity that historically enjoyed a constitutionally protected privacy interest, Supreme Court precedent can be viewed as supporting the notion that the historically protected privacy interest must trump the third-party doctrine for purposes of Fourth Amendment analysis. If the historically protected privacy interest does not, then with every new technology, we surrender more and more of our historically protected Fourth Amendment interests to unreasonable searches and seizures.

MARTIN, Circuit Judge, dissenting,<sup>1</sup> in which JILL PRYOR, Circuit Judge, joins:

In this case, the government got 67 days of cell site location data disclosing Quartavious Davis's location every time he made or received a call on his cell phone. It got all this without obtaining a warrant. During that time, Mr. Davis made or received 5,803 phone calls, so the prosecution had 11,606 data points about Mr. Davis's location. We are asked to decide whether the government's actions violated Mr. Davis's Fourth Amendment rights. The majority says our analysis is dictated by the third-party doctrine, a rule the Supreme Court developed almost forty years ago in the context of bank records and telephone numbers. But such an expansive application of the third-party doctrine would allow the government warrantless access not only to where we are at any given time, but also to whom we send e-mails, our search-engine histories, our online dating and shopping records, and by logical extension, our entire online personas.

---

<sup>1</sup> The en banc court voted to vacate the panel opinion which held that the warrantless search of Mr. Davis's cell site location data was unconstitutional, but upheld Mr. Davis's conviction based on the good-faith exception. The good-faith exception says that where officers' conduct is based on their good-faith understanding of an existing statute, the exclusionary rule will not apply. See, e.g., United States v. Williams, 622 F.2d 830, 843 (5th Cir. 1980); see also Bonner v. City of Prichard, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc) (adopting as binding precedent all decisions of the former Fifth Circuit handed down before October 1, 1981). The majority here refers to the good-faith exception as an alternative basis for affirming Mr. Davis's conviction. Maj. Op. 44 n.20. I agree with them about that. My disagreement is with the majority's Fourth Amendment analysis, which permits government access to Mr. Davis's cell site location data without a warrant. I understand the Fourth Amendment to require the government to get a warrant for that information, while the majority does not. I refer to this opinion as a dissent, not a concurrence in the judgment, for that reason.

Decades ago, the Supreme Court observed that “[i]f times have changed, reducing everyman’s scope to do as he pleases in an urban and industrial world, . . . the values served by the Fourth Amendment [are] more, not less, important.” Coolidge v. New Hampshire, 403 U.S. 443, 455, 91 S. Ct. 2022, 2032 (1971). This is even truer today. The judiciary must not allow the ubiquity of technology—which threatens to cause greater and greater intrusions into our private lives—to erode our constitutional protections. With that in mind, and given the striking scope of the search in this case, I would hold that the Fourth Amendment requires the government to get a warrant before accessing 67 days of the near-constant cell site location data transmitted from Mr. Davis’s phone. I respectfully dissent.

# I.

I turn first to the third-party doctrine, which the majority believes decides this case for us. They say: “Davis can assert neither ownership nor possession of the third-party’s business records he sought to suppress.” Maj. Op. 27; see also William Pryor Concurrence 45 (“Smith controls this appeal.”). My reading of Supreme Court precedent suggests that things are not so simple.

The Supreme Court announced the third-party doctrine nearly forty years ago in United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619 (1976). The Court said that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if

the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.” Id. at 443, 96 S. Ct. at 1624. Three years later, in Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577 (1979), the Court applied that doctrine to hold that a defendant did not have a reasonable expectation of privacy in the numbers he dialed on his home telephone, recorded by means of a pen register at a telephone company’s central office. Id. at 742, 99 S. Ct. at 2581. The Court reasoned that “[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business.” Id. at 744, 99 S. Ct. at 2582. The Court reminisced that “[t]he switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.” Id. The government believes that Smith controls the outcome of this case, and the majority apparently agrees. I do not.

First, the phone numbers a person dials are readily distinguishable from cell site location data. Smith involved “voluntarily conveyed numerical information”—voluntary because phone dialers have to affirmatively enter the telephone number they are dialing in order to place a call. By contrast, cell phone users do not affirmatively enter their location in order to make a call. Beyond that, the ACLU informs us that “[p]hones communicate with the wireless network when

a subscriber makes or receives calls.” ACLU Amicus Br. 5 (emphasis added). As our sister Circuit observed, “when a cell phone user receives a call, he hasn’t voluntarily exposed anything at all.” In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t, 620 F.3d 304, 317–18 (3d Cir. 2010) (Third Circuit Case) (emphasis added) (quotation marks omitted).<sup>2</sup>

The Smith Court also emphasized that the numbers a person dials appear on the person’s telephone bill and referenced the pre-automation process that required the caller to recite phone numbers out loud to a phone operator in order to make a call. Thus, the Court concluded that “[t]elephone users . . . typically know that they must convey numerical information to the phone company.” Smith, 442 U.S. at 743, 99 S. Ct. at 2581 (emphasis added). There is not the same sort of “knowing” disclosure of cell site location data to phone companies because there is

---

<sup>2</sup> The majority extensively recounts the Fifth Circuit’s decision in In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013), which said that a “cell user ha[s] no subjective expectation of privacy in such business records showing cell tower locations.” Maj. Op. 25. That Fifth Circuit case, of course, does not bind us. And in any event, other courts have held that people do have a reasonable expectation of privacy in cell site location data, whether historical or real-time in nature. The Third Circuit Case, for example, rejected the government’s argument that “no [cell site location data] can implicate constitutional protections because the subscriber has shared its information with a third party. . . .” 620 F.3d at 317. Similarly, the Florida Supreme Court has held that cell phone users have a reasonable expectation of privacy in real-time cell site location data. Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014). And a recent decision from the Northern District of California addressed the very same question we address here and held that a person has a reasonable expectation of privacy in 60 days of historical cell site location data. United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL 881578, at \*6–8 (N.D. Cal. Mar. 2, 2015). In short, we are faced with persuasive, albeit not binding, authority on both sides of the debate, but none controls the outcome of this case.

no history of cell phone users having to affirmatively disclose their location to an operator in order to make a call. The extent of voluntariness of disclosure by a user is simply lower for cell site location data than for the telephone numbers a person dials. For that reason, I don't think Smith controls this case.

Second, although the Miller/Smith rule appears on its own to allow government access to all information that any third-party obtains, in rulings both before and since those cases, the Supreme Court has given reasons to doubt the rule's breadth. For instance, in Ferguson v. City of Charleston, 532 U.S. 67, 121 S. Ct. 1281 (2001), the Court stated that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." Id. at 78, 121 S. Ct. at 1288. Though the majority did not mention the third-party doctrine, Justice Scalia noted the incongruity between that doctrine and the Ferguson holding in his dissent. As he stated:

Until today, we have never held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain. Without so much as discussing the point, the Court today opens a hole in our Fourth Amendment jurisprudence, the size and shape of which is entirely indeterminate.

Id. at 95–96, 121 S. Ct. at 1297–98 (Scalia, J., dissenting). Further, and again without mentioning the third-party doctrine, the Court has routinely recognized that people retain a reasonable expectation of privacy in things that they have



arguably exposed to third parties. See, e.g., United States v. Jacobsen, 466 U.S. 109, 114, 104 S. Ct. 1652, 1657 (1984) (holding that “[l]etters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy” even though they touch the hands of third-party mail carriers); Stoner v. California, 376 U.S. 483, 487–88, 490, 84 S. Ct. 889, 892, 893 (1964) (finding unpersuasive the argument that “the search of [a] hotel room, although conducted without the petitioner’s consent, was lawful because it was conducted with the consent of the hotel clerk,” because a hotel guest’s constitutional protections should not be “left to depend on the unfettered discretion of an employee of the hotel”); see also Smith, 442 U.S. at 746–47, 99 S. Ct. at 2583 (Stewart, J., dissenting) (noting that in Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967), the Court held that a person has a reasonable expectation of privacy in the contents of phone conversations made in telephone booths even though calls “may be recorded or overheard by the use of other company equipment”). I am well aware that each of these cases can be distinguished from Mr. Davis’s case. I mean only to say that a comprehensive review of Supreme Court precedent reveals that the third-party doctrine may not be as all-encompassing as the majority seems to believe.

Third and most importantly, the majority’s blunt application of the third-party doctrine threatens to allow the government access to a staggering amount of

information that surely must be protected under the Fourth Amendment. Consider the information that Google gets from users of its e-mail and online search functions.<sup>3</sup> According to its website, Google collects information about you (name, e-mail address, telephone number, and credit card data); the things you do online (what videos you watch, what websites you access, and how you view and interact with advertisements); the devices you use (which particular phone or computer you are searching on); and your actual location. See Privacy Policy, <http://www.google.com/intl/en/policies/privacy/> (last accessed March 30, 2015). Beyond that, in its “Terms of Service,” Google specifies that “[w]hen you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works, . . . communicate, publish, publicly perform, publicly display and distribute such content.” See Google Terms of Service, <http://www.google.com/intl/en/policies/terms/> (last accessed March 30, 2015). Like in Miller and Smith, Google even offers a legitimate business purpose for such data storage and mining: “Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection.” Id. Under a plain reading of the majority’s rule, by allowing a third-party company

---

<sup>3</sup> I refer to Google only as an example. The same analysis applies to most other online search engine or e-mail service providers.

access to our e-mail accounts, the websites we visit, and our search-engine history—all for legitimate business purposes—we give up any privacy interest in that information.

And why stop there? Nearly every website collects information about what we do when we visit. So now, under the majority’s rule, the Fourth Amendment allows the government to know from YouTube.com what we watch, or Facebook.com what we post or whom we “friend,” or Amazon.com what we buy, or Wikipedia.com what we research, or Match.com whom we date—all without a warrant. In fact, the government could ask “cloud”-based file-sharing services like Dropbox or Apple’s iCloud for all the files we relinquish to their servers. I am convinced that most internet users would be shocked by this. But as far as I can tell, every argument the government makes in its brief regarding cell site location data applies equally well to e-mail accounts, search-engine histories, shopping-site purchases, cloud-storage files, and the like. See, e.g., Appellee’s Br. 21–22 (“Davis can assert neither ownership nor possession of the third-party records he sought to suppress.”); id. at 22 (“Evidence lawfully in the possession of a third party is not his, even if it has to do with him.”); id. at 23 (“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.”); id. at 24 (“It is not persuasive to argue that phone users do

not knowingly or intentionally disclose any location-related information to their service providers.”); id. at 25 (“For purposes of the Fourth Amendment, it makes no difference whether Davis knew that MetroPCS was collecting location-related information.”); id. at 27–28 (“[S]ervice 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.”).

The enormous impact of this outcome is probably why at least one Circuit has held that a person’s Fourth Amendment rights are violated when the government compels an internet service provider to turn over the contents of e-mails without a warrant. See United States v. Warshak 631 F.3d 266, 286–88 (6th Cir. 2010). Surely the majority would agree and would also shield e-mails from government snooping absent a warrant. But if e-mails are protected despite the fact that we have surrendered control of them to a third party, then the rule from Smith and Miller has its limits.

The majority suggests that e-mails can be distinguished because cell site location data is “non-content evidence.” Maj. Op. 27 (emphasis omitted). The majority offers no coherent definition of the terms “content” and “non-content,” and I am hard-pressed to come up with one. For instance, would a person’s Google search history be content or non-content information? Though a person’s search terms may seem like “content,” a search term exists in the web address

generated by a search engine.<sup>4</sup> And web addresses, like phone numbers, seem like quintessentially non-content information that merely direct a communication. But regardless, although this content–non-content distinction could—maybe—shield the body of e-mail messages, the government may presumably still access the time and date that we send e-mails, the names of the people who receive them, and the names of the people who email us, without a warrant. Likewise, although our actual activities on a dating or shopping website might be protected, the fact that we visited those websites or any other would still be freely discoverable. The government agreed at oral argument that under its theory, it could at the very least obtain records like the sender and receiver of e-mails, the time of day e-mails are sent, the number of e-mails a person sends, the websites that a person visits, and maybe even the connections a person communicates with on a dating website and whom she meets in person—all without a warrant.

This slippery slope that would result from a wooden application of the third-party doctrine is a perfect example of why the Supreme Court has insisted that technological change sometimes requires us to consider the scope of decades-old Fourth Amendment rules. See Kyllo v. United States, 533 U.S. 27, 35, 121 S. Ct. 2038, 2044 (2001) (rejecting a “mechanical interpretation of the Fourth Amendment” in the face of “advancing technology”); cf. Katz, 389 U.S. at 353, 88

---

<sup>4</sup> For example, a search of “Eleventh Circuit” on google.com produces the web address: “[https://www.google.com/?gws\\_rd=ssl#q=eleventh+circuit](https://www.google.com/?gws_rd=ssl#q=eleventh+circuit).”

S. Ct. at 512 (“To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”). For instance, in Riley v. California, 573 U.S. \_\_\_, 134 S. Ct. 2473 (2014), the Court was asked to decide whether the decades-old search-incident-to-arrest exception to the warrant requirement applied to cell phones on an arrestee’s person. Id. at 2480. California argued that the Court’s 41-year-old decision in United States v. Robinson, 414 U.S. 218, 94 S. Ct. 467 (1973), controlled the outcome in Riley because the Court held that a search of objects on an arrestee’s person was categorically reasonable. See Riley, 134 S. Ct. at 2491. The Riley Court agreed that “a mechanical application of Robinson might well support the warrantless searches at issue.” Id. at 2484. But it nonetheless unanimously rejected that argument, saying that cell “phones are based on technology nearly inconceivable just a few decades ago, when . . . Robinson w[as] decided.” Id. Thus, to say that a search of cell phone data is “materially indistinguishable” from a search of physical items

is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.

Id. at 2488–89.

Likewise here, the extent of information that we expose to third parties has

increased by orders of magnitude since the Supreme Court decided Miller and Smith. Those forty years have seen not just the proliferation of cell phones that can be tracked, but also the advent of the internet. Given these extraordinary technological advances, I believe the Supreme Court requires us to critically evaluate how far to extend the third-party doctrine. As Justice Sotomayor observed:

[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

United States v. Jones, 565 U.S. \_\_\_, \_\_\_, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted). Neither would I assume as much. Though the doctrine may allow the government access to some information that we disclose to third parties, I would draw the line short of the search at issue here. Sixty-seven days of near-constant location tracking of a cell phone—a technological feat impossible to imagine when Miller and Smith were decided—is an application of the doctrine that goes too far.

## II.

Because I believe that the third-party doctrine does not dictate the outcome of this case, I turn to fundamental Fourth Amendment principles. The Fourth

Amendment says:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. “As the text makes clear, the ultimate touchstone of the Fourth Amendment is reasonableness.” Riley, 134 S. Ct. at 2482 (quotation marks omitted). Our analysis is two-fold: “First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that he sought to preserve something as private.” Bond v. United States, 529 U.S. 334, 338, 120 S. Ct. 1462, 1465 (2000) (quotation omitted) (alteration adopted). “Second, we inquire whether the individual’s expectation of privacy is one that society is prepared to recognize as reasonable.” Id. (quotation omitted). If we conclude that a particular search violates a defendant’s reasonable expectation of privacy, the government must get a search warrant.

For me, the answer to the subjective inquiry is easy. It seems obvious that Mr. Davis never intended to disclose his location to the government every time he made or received calls. Recent polling data tells us that 82% of adults “feel as though the details of their physical location gathered over a period of time” is “very sensitive” or “somewhat sensitive.” Mary Madden, Public Perceptions of Privacy and Security in the Post-Snowden Era 34, Pew Research Center (Nov. 12,



2014), [http://www.pewinternet.org/files/2014/11/PI\\_PublicPerceptionsofPrivacy\\_111214.pdf](http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf). This supports the common-sense notion that people do not expect the government to track them simply as a consequence of owning and using what amounts to a basic necessity of twenty-first century life—the cell phone.<sup>5</sup> Beyond that, the prosecutor in this case specifically admitted at closing argument that “what this defendant could not have known was that . . . his cell phone was tracking his every moment.” Trial Tr. 4–5, Feb. 8, 2012, ECF No. 287 (emphasis added); see also id. at 14 (arguing that Mr. Davis and his co-conspirators “had no idea that by bringing their cell phones with them to these robberies they were allowing MetroPCS and now [the jury] to follow their movements”). In short, I believe that Mr. Davis—like any other person interacting in today’s digital world—quite reasonably had a subjective expectation that his movements about town would be kept private.<sup>6</sup>

---

<sup>5</sup> The government argues that regardless of what people think, “MetroPCS’s current privacy policy . . . 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.’” Appellee Br. 28 (citation omitted). But as another court recently noted, “[t]he fiction that the vast majority of the American population consents to warrantless government access to the records of a significant share of their movements by ‘choosing’ to carry a cell phone must be rejected.” In re Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 127 (E.D.N.Y. 2011). Regardless, and as the majority acknowledges, the “contract does not appear on this record to have been entered into evidence here,” so “we cannot consider it.” Maj. Op. 25 n.11.

<sup>6</sup> The majority does not explain why it believes that “the fact that Davis registered his cell phone under a fictitious alias tends to demonstrate his understanding that such cell tower location information is collected by MetroPCS and may be used to incriminate him.” Maj. Op. 28. Mr. Davis’s use of an alias more naturally evidences his desire not to tie his identity to his phone’s

The more important and more difficult question we must consider is whether Mr. Davis's expectation of privacy is one society is objectively prepared to recognize as reasonable. I believe the answer is yes. The Supreme Court recently reminded us that "there is an element of pervasiveness that characterizes cell phones." Riley, 134 S. Ct. at 2490. Today, "it is the person who is not carrying a cell phone . . . who is the exception." Id. The Court noted that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower." Id. (quoting Harris Interactive, 2013 Mobile Consumer Habits Study (June 2013)). In other words, "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." Id. at 2484; see also City of Ontario, Cal. v. Quon, 560 U.S. 746, 760, 130 S. Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

Since we constantly carry our cell phones, and since they can be used to track our movements, the recent opinions of five Justices in United States v. Jones that long-term location-monitoring generally violates expectations of privacy are

---

account with MetroPCS. For me, Mr. Davis's use of an alias says nothing about his subjective expectation of privacy in his location.

instructive. In Jones, the Supreme Court considered whether warrantless monitoring of the location of a person's car for twenty-eight days by means of a GPS tracker violated the defendant's rights under the Fourth Amendment. 132 S. Ct. at 948–49. All nine Justices said yes. Five Justices held that such tracking violated the Fourth Amendment under a trespass theory that considered the government's physical intrusion of the car. Id. at 949. Important for Mr. Davis's case, however, a different set of five Justices were in agreement that “longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” Id. at 955 (Sotomayor, J., concurring) (quoting id. at 964 (Alito, J., joined by Ginsburg, Breyer, and Kagan, JJ., concurring in the judgment)). Said one Justice, “GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.” Id. at 955 (Sotomayor, J., concurring). Said four other Justices, “society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.” Id. at 964 (Alito, J., concurring in the judgment).<sup>7</sup>

The search at issue here similarly impinged on expectations of privacy. The

---

<sup>7</sup> The majority chides Mr. Davis for “deploy[ing] the concurrences in Jones,” Maj. Op. 33, but a lower federal court ignores the opinion of five Justices of the Supreme Court at its own risk.

location data the government collected, though not quite as precise as the GPS data in Jones, still revealed Mr. Davis's comings and goings around Miami with an unnerving level of specificity. Each time he made or received a call, MetroPCS catalogued the cell tower to which his cell phone connected, typically the "[n]earest and strongest" tower. Trial Tr. 221, Feb. 6, 2012, ECF No. 283. In a "cosmopolitan area [like] Miami," there are "many, many towers" whose coverage radii are "much smaller" than a "mile-and-a-half." Id. at 222–23. Each coverage circle is further subdivided into "three or six portions." Id. at 222. The data the government obtained in this case specified the sector within a tower's coverage radius in which Mr. Davis made or received a call.

The amount of data the government got is also alarming. The government demanded from MetroPCS sixty-seven days of cell site location data—more than double the time at issue in Jones. In total, this data included 5,803 separate call records. Since MetroPCS cataloged the cell tower sector where each phone call started and ended, the government had 11,606 cell site location data points. This averages around one location data point every five and one half minutes for those sixty-seven days, assuming Mr. Davis slept eight hours a night.

The amount and type of data at issue revealed so much information about Mr. Davis's day-to-day life that most of us would consider quintessentially private. For instance, on August 13, 2010, Mr. Davis made or received 108 calls in 22

unique cell site sectors, showing his movements throughout Miami during that day. And the record reflects that many phone calls began within one cell site sector and ended in another, exposing his movements even during the course of a single phone call.

Also, by focusing on the first and last calls in a day, law enforcement could determine from the location data where Mr. Davis lived, where he slept, and whether those two locations were the same. As a government witness testified at trial, “if you look at the majority of . . . calls over a period of time when somebody wakes up and when somebody goes to sleep, normally it is fairly simple to decipher where their home tower would be.” Trial Tr. 42, Feb. 7, 2012, ECF No. 285. For example, from August 2, 2010, to August 31, 2010, Mr. Davis’s first and last call of the day were either or both placed from a single sector—purportedly his home sector. But on the night of September 2, 2010, Mr. Davis made calls at 11:41pm, 6:52am, and 10:56am—all from a location that was not his home sector. Just as Justice Sotomayor warned, Mr. Davis’s “movements [were] recorded and aggregated in a manner that enable[d] the Government to ascertain, more or less at will, . . . [his] sexual habits, and so on.” Jones, 132 S. Ct. at 956 (Sotomayor, J., concurring); see also United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (“A person who knows all of another’s travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband,

an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.”).

Importantly, the specificity of the information that the government obtained was highlighted by the way the government used it at trial. The government relied upon the information it got from MetroPCS to specifically pin Mr. Davis’s location at a particular site in Miami. See, e.g., Trial Tr. 58, Feb. 7, 2012, ECF No. 285 (noting that “Mr. Davis’s phone [was] literally right up against the America Gas Station immediately preceding and after [the] robbery occurred”); id. at 61 (noting “the presence of his cell phone literally . . . right next door to the Walgreen’s just before and just after that store was robbed”). On this record, Mr. Davis had a reasonable expectation of privacy in the cell site location data the government obtained, and his expectation was one that society should consider reasonable. I would therefore hold that absent a warrant, a Fourth Amendment violation occurred.

### III.

The majority, of course, believes that Mr. Davis had no reasonable expectation of privacy in the cell site location data obtained in his case. It emphasizes the large size of the sectors that each location data point revealed as evidence that the privacy intrusion was not so great. See Maj. Op. 5–6, 10–12. It also says we need not consider more invasive technologies that have developed

since the search that took place here. Id. at 11 n.7 (“There is no evidence, or even any allegation, that the MetroPCS network reflected in the records included anything other than traditional cell towers and the facts of this case do not require, or warrant, speculation as to the newer technology.”). Yet the Supreme Court has cautioned us that “[w]hile the technology used in the present case [may be] relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development.” Kyllo, 533 U.S. at 36, 121 S. Ct. at 2044. Just as the majority appropriates decades-old precedent from Miller and Smith and applies it to new technologies, the rule we make today necessarily will apply to everyone else’s case going forward.

That future impact is troubling. As technology advances, the specificity of cell site location information has increased. Cell phone companies are constantly upgrading their networks with more and more towers. As the ACLU explains:

Cell site density is increasing rapidly, largely as a result of the growth of internet usage by smartphones. . . . As new cell sites are erected, the coverage areas around existing nearby cell sites will be reduced, so that the signals sent by those sites do not interfere with each other. In addition to erecting new conventional cell sites, providers are also increasing their network coverage using low-power small cells, called “microcells,” “picocells,” and “femtocells” (collectively, “femtocells”), which provide service to areas as small as ten meters. . . . Because the coverage area of femtocells is so small, callers connecting to a carrier’s network via femtocells can be located to a high degree of precision, sometimes effectively identifying individual floors and rooms within buildings.

ACLU Amicus Br. 7–8 (quotations, citations omitted); see also id. at 7 (noting that

“the number of cell sites in the United States has approximately doubled in the last decade”); id. at 8 (noting that “[f]emtocells with ranges extending outside of the building in which they are located can also provide cell connections to passersby, providing highly precise information about location and movement on public streets and sidewalks”). The location features on smartphones are even more precise. See Riley, 134 S. Ct. at 2490 (“Historic location information is a standard feature on many smart phones and can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.”).

Beyond that, today, the vast majority of communications from cell phones are in the form of text messages and data transfers, not phone calls. The frequency of text messaging is much greater than the frequency of phone calling—particularly among young cell phone users. See Amanda Lenhart, Teens, Smartphones & Texting (available at <http://www.pewinternet.org/2012/03/19/teens-smartphones-texting/>) (finding that the median number of texts sent per day by teens ages 12 to 17 rose from 50 in 2009 to 60 in 2011). Also, “smartphones, which are now used by more than six in ten Americans, communicate even more frequently with the carrier’s network, because they typically check for new email messages or other data every few minutes.” ACLU Amicus Br. 5 (citations omitted). Each of these new types of communications can generate cell site location data. See, e.g., United States v. Cooper, No. 13-cr-00693-SI-1, 2015 WL



881578, at \*8 n.6 (N.D. Cal. Mar. 2, 2015) (noting the government’s admission that “cell site data is recorded for both calls and text messages”).

Finally, not only are cell sites fast growing in number, but the typical user has no idea how precise cell site location data is at any given location. As a person walks around town, particularly a dense, urban environment, her cell phone continuously and without notice to her connects with towers, antennas, microcells, and femtocells that reveal her location information with differing levels of precision—to the nearest mile, or the nearest block, or the nearest foot. And since a text or phone call could come in at any second—without any affirmative act by a cell phone user—a user has no control over the extent of location information she reveals.

The government tells us these technological advances do not change our analysis. At oral argument, it admitted that its theory requires us to hold that it could obtain location data without a warrant even when technology someday allows it to know a person’s location to within six inches, and when tracking is continuous and does not require making or receiving a phone call. I reject a theory that allows the government such expansive access to information about where we are located, no matter how detailed a picture of our movements the government may receive.

But we need not fear the threat of increasing precision of location

information, says the majority. At the same time it suggests that today's ruling might not apply to future technology, however, the majority's opinion offers absolutely no guidance to the judges who authorize searches of cell site location data and the officers who conduct them. As the ACLU pointed out, "[a]gents will not have prior knowledge of whether the surveillance target was in a rural area with sparse cell sites, an urban area with dense cell sites or six-sector antennas, or a home, doctor's office, or church with femtocells." ACLU Amicus Br. 9. Thus, a judge will authorize a search of a person's cell site location data for a certain period of time without knowing how precise the location information will be. While I admire the majority's attempt to cabin its holding to the technology of five years ago, its assurances in this regard seem naïve in practice. As a result of today's decision, I have little doubt that all government requests for cell site location data will be approved, no matter how specific or invasive the technology.

#### IV.

The majority offers dire warnings of the consequences of restricting the government's access to cell site location data, suggesting that without it, all manner of horrific crimes—from child abductions to terrorism—would go uninvestigated. See Maj. Op. 42. But if my view of the Fourth Amendment were to prevail, all the officers in this case had to do was get a warrant for this search. That is no great burden. "Under the Fourth Amendment, an officer may not

properly issue a warrant . . . unless he can find probable cause therefor from facts or circumstances presented to him under oath or affirmation.” Nathanson v. United States, 290 U.S. 41, 47, 54 S. Ct. 11, 13 (1933). The probable-cause standard is not onerous. See Illinois v. Gates, 462 U.S. 213, 291, 103 S. Ct. 2317, 2360 (1983) (Brennan, J., dissenting) (criticizing a probable-cause standard that “imposes no structure on magistrates’ probable cause inquiries . . . and invites the possibility that intrusions may be justified on less than reliable information from an honest or credible person”); Ricardo J. Bascuas, Property and Probable Cause: The Fourth Amendment’s Principled Protection of Privacy, 60 Rutgers L. Rev. 575, 592–93 (2008) (“The Supreme Court has set the standard for the quality of information that can support a warrant so low that judges can hardly be expected to uncover a baseless request.”); cf. Riley, 134 S. Ct. at 2493 (noting that “[r]ecent technological advances . . . have . . . made the process of obtaining a warrant itself more efficient”). Nor is cell site data the type of information which would spoil or perish during the short time it takes to get a warrant. Finally, requiring a warrant would not do away with the other well-established exceptions to the warrant requirement, like exigent circumstances. Cf. Riley, 134 S. Ct. at 2494 (noting that “the availability of the exigent circumstances exception . . . address[es] some of the more extreme hypotheticals that have been suggested”). Imposing the requirement for a warrant under these circumstances would hardly shackle law enforcement

from conducting effective investigations.

But regardless of how easy it might be to get warrants, the Supreme Court has reminded us time and again of how important they are.

The warrant requirement has been a valued part of our constitutional law for decades, and it has determined the result in scores and scores of cases in courts all over this country. It is not an inconvenience to be somehow ‘weighed’ against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the ‘well-intentioned but mistakenly over-zealous, executive officers’ who are a part of any system of law enforcement.

Coolidge, 403 U.S. at 481, 91 S. Ct. at 2046 (citation omitted). The majority emphasizes that the Stored Communications Act (SCA) requires the government to “offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d). But it does not contest—nor could it—that this standard falls below the probable-cause standard that courts usually demand. See Maj. Op. 15.<sup>8</sup>

Once again, the Supreme Court’s analysis in Riley is instructive.<sup>9</sup> There, the

---

<sup>8</sup> Certainly the Stored Communications Act is better than nothing. See Maj. Op. 15 (noting that the SCA “raises the bar from an ordinary subpoena to one with additional privacy protections built in”). But the mere fact that the Act provides some judicial oversight before the government can get cell site location data does not answer the question whether the government is constitutionally required to have a warrant.

<sup>9</sup> “[T]here is dicta and then there is dicta, and then there is Supreme Court dicta.” Schwab v. Crosby, 451 F.3d 1308, 1325 (11th Cir. 2006).

Court recognized:

We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost.

Riley, 134 S. Ct. at 2493. But still, the Court insisted that law enforcement officers get a warrant before searching a cell phone incident to arrest. So too here. I would simply require the government do what it has done for decades when it seeks to intrude upon a reasonable expectation of privacy. That is, “get a warrant.” Id. at 2495.

V.

The majority proclaims that its holding today is “narrow[],” Maj. Op. 14, limited only to cell site location data, and only to the kind of data the government could obtain in 2010. But “[s]teps innocently taken may one by one lead to the irretrievable impairment of substantial liberties.” Glasser v. United States, 315 U.S. 60, 86, 62 S. Ct. 457, 472 (1942). Under the reasoning employed by the majority, the third-party doctrine may well permit the government access to our precise location at any moment, and in the end, our entire digital lives. And although Mr. Davis—as the majority reminds us in great detail, see Maj. Op. 3–5—has been convicted of very serious crimes and is not therefore the most

sympathetic bearer of this message,<sup>10</sup> “the rule[s] we fashion [are] for the innocent and guilty alike.” Draper v. United States, 358 U.S. 307, 314, 79 S. Ct. 329, 333 (1959) (Douglas, J., dissenting). I would not subject the citizenry to constant location tracking of their cell phones without requiring the government to get a warrant. The Fourth Amendment compels this result. I respectfully dissent.

---

<sup>10</sup> Though regardless of the outcome of this en banc appeal, Mr. Davis’s convictions will stand and he will remain incarcerated due to the good-faith exception. See supra note 1.