No. 16-402

In the Supreme Court of the United States

TIMOTHY IVORY CARPENTER, PETITIONER

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES

NOEL J. FRANCISCO
Solicitor General
Counsel of Record
KENNETH A. BLANCO
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
ELIZABETH B. PRELOGAR
Assistant to the Solicitor General
JENNY C. ELLICKSON
Attorney

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the government's acquisition, pursuant to a court order issued under 18 U.S.C. 2703(d), of historical cell-site records created and maintained by a cell-service provider violates the Fourth Amendment rights of the individual customer to whom the records pertain.

TABLE OF CONTENTS

Page

Table of Contents—Continued: Page

TABLE OF FIGURES

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Cases—Continued: Page

Cases—Continued: Page

Constitution and statutes:

Statutes—Continued: Page

Miscellaneous:

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 16-402

TIMOTHY IVORY CARPENTER, PETITIONER

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF FOR THE UNITED STATES

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-32a) is reported at 819 F.3d 880. The opinion and order of the district court denying petitioner's motion to suppress (Pet. App. 34a-48a) is not published in the Federal Supplement but is available at 2013 WL 6385838.

JURISDICTION

The judgment of the court of appeals was entered on April 13, 2016. A petition for rehearing was denied on June 29, 2016 (Pet. App. 33a). The petition for a writ of certiorari was filed on September 26, 2016. This Court's jurisdiction rests on 28 U.S.C. 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Relevant provisions are reprinted in Appendix A, *infra*, 1a-12a.

STATEMENT

Following a jury trial in the United States District Court for the Eastern District of Michigan, petitioner was convicted on six counts of aiding and abetting Hobbs Act robbery, in violation of 18 U.S.C. 1951(a), and five counts of aiding and abetting the use or carrying of a firearm during and in relation to a crime of violence, in violation of 18 U.S.C. 924(c). Pet. App. 5a-6a. The district court sentenced petitioner to 1395 months in prison. *Id.* at 7a. The court of appeals affirmed. *Id.* at 1a-32a.

A. Cell-Site Records And The Stored Communications Act

1. Cellular telephones "work by establishing a radio connection with nearby cell towers (or 'cell sites')." Pet. App. 5a; see *id.* at 76a-77a. "[A] cell tower is a large antenna that emits a radio frequency" to cell phones within the tower's coverage area. J.A. 45. "[I]ndividual towers project different signals in each direction or 'sector,'" typically with three sectors per tower. Pet. App. 5a, 78a; J.A. 45. If a provider does not have towers covering a particular area, the provider may enter into a "roaming" agreement to use another provider's towers. J.A. 44; see J.A. 49-50, 63-64. In rural areas, "a tower's coverage might reach as far as 20 miles." Pet. App. 5a. "In an urban area like Detroit," where most of the robberies at issue occurred, "each cell site covers typically anywhere from a half-mile to two miles." *Ibid.* (internal quotation marks omitted).

When an individual places or receives a call on a cell phone, the phone scans its environment and connects to the cell site with the best signal, which will typically be the tower closest to the phone or in its direct line of sight. Pet. App. 76a-77a. Factors other than distance

may influence signal strength, including "buildings, topography," and "[t]he time of year." J.A. 48. During the call, the phone and tower transmit signals to each other to maintain the connection, and the phone may switch to a new tower if the signal strength fluctuates or the phone moves. J.A. 43-44, 83; Pet. App. 77a.

Cell-service providers "typically log and store certain call-detail records of their customers' calls, including the date, time, and length of each call; the phone numbers engaged on the call; and the cell sites where the call began and ended." Pet. App. 5a-6a. No law requires providers to create or maintain cell-site records; instead, providers retain those records in the ordinary course of business for their own purposes. *Id.* at 7a, 10a. Those purposes include finding weak spots in the providers' networks and applying roaming charges. *Ibid.* In addition, providers may sell aggregated cell-site data they collect or otherwise use that data in business ventures unrelated to providing cell-phone service. See, *e.g.*, Electronic Privacy Information Center (EPIC) Amicus Br. 22-23 (describing how cell-service providers sell location data to data brokers); Tech. Experts Amicus Br. 23 (stating that providers have "found commercial uses for location data"). Providers in the United States disclose their collection and use of cell-site data in their privacy policies.[1]

---

[1] See, *e.g.*, Verizon, *Privacy Policy* (June 2017), http://www.verizon.com/about/privacy/full-privacy-policy ("Verizon Wireless collects and uses mobile device location data for a variety of purposes."); AT&T, *AT&T Privacy Policy* (May 2, 2017), http://about.att.com/sites/privacy_policy/full_privacy_policy (explaining that AT&T collects and uses "[l]ocation information [that] is generated when [users'] device[s] communicate[] with cell towers"); Sprint, *Sprint Corporation Privacy Policy* (Mar. 29, 2017), https://www.sprint.com/legal/privacy.html (informing users that Sprint "may

2. The Stored Communications Act (SCA), 18 U.S.C. 2701 *et seq.*, authorizes the government to obtain cell-service providers' records pertaining to their subscribers under specified circumstances. 18 U.S.C. 2703. As relevant here, the government may require a provider "to disclose a record or other information pertaining to a subscriber * * * (not including the contents of communications)" through "a court order for such disclosure under [18 U.S.C. 2703(d)]." 18 U.S.C. 2703(c)(1)(B). To obtain a Section 2703(d) order, the government must "offer[] 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). On the provider's motion, the court "may quash or modify [a Section 2703(d)] order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden." *Ibid.* In addition, a provider may raise a Fourth Amendment challenge to a Section 2703(d) order, to ensure compliance with constitutional limits on the use of compulsory process. See *Donovan* v. *Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) ("[T]he Fourth Amendment requires that [a] subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.") (citation omitted).

---

collect information about * * * [their] location" and use that information in a variety of circumstances); T-Mobile, *T-Mobile Privacy Policy* (Dec. 31, 2016), https://www.t-mobile.com/company/website/privacypolicy.aspx#fullpolicy (stating that T-Mobile's "systems capture details about the * * * location of wireless device[s] [customers] use").

B. The Present Controversy

1. Beginning in December 2010, petitioner and his co-conspirators committed a string of armed robberies at Radio Shack and T-Mobile stores in Ohio and Michigan. Pet. App. 3a, 6a. Petitioner typically organized the robberies, supplied the guns, and acted as a lookout. *Id.* at 5a. On petitioner's signal, a group of robbers "entered the store, brandished their guns, herded customers and employees to the back, and ordered the employees to fill the robbers' bags with new smartphones." *Ibid.* After each robbery, the team met nearby to dispose of the guns and getaway vehicle and sell the stolen merchandise. *Ibid.*

2. a. In April 2011, police arrested four of petitioner's co-conspirators, and one of them "confessed that the group had robbed nine different stores in Michigan and Ohio between December 2010 and March 2011, supported by a shifting ensemble of 15 other men who served as getaway drivers and lookouts." Pet. App. 3a. Based on that information, the government applied to federal magistrate judges for court orders pursuant to Section 2703(d) of the SCA. *Id.* at 3a-4a; see *id.* at 49a-55a, 62a-68a. As relevant here, those applications sought orders directing MetroPCS and Sprint to disclose non-content records for a cell-phone number that petitioner used, including "cell site information for [petitioner's] telephone[] at call origination and at call termination for incoming and outgoing calls." *Id.* at 4a. Specifically, the government requested 152 days of historical cell-site records from MetroPCS, spanning the period when the string of robberies occurred in Detroit between December 2010 and April 2011. *Id.* at 52a, 61a. The government sought seven days of records from Sprint, linked to the date of a robbery in Warren, Ohio,

where MetroPCS has a roaming agreement with Sprint. *Id.* at 65a, 80a.

The magistrate judges issued the requested orders. Pet. App. 4a; see *id.* at 56a-61a, 69a-73a. MetroPCS then produced 127 days of cell-site records and Sprint produced two days of records for petitioner's phone number. *Id.* at 7a; Pet. Br. 7. The records showed the towers petitioner's phone connected to when it made and received calls, but did not contain any cell-site information for text messages or for times when petitioner's phone was turned on but was not being used to connect a call. See Pet. App. 7a.

From the cell-site records, as well as MetroPCS and Sprint records identifying the locations of their towers, the government could infer the approximate location of petitioner's phone when calls were connected to it around the time of the robberies. Pet. App. 6a; J.A. 78-79. Because the cell sites covered areas "extending between one-half mile and two miles in length," however, the government could determine the location of petitioner's phone only "within a 3.5 million square-foot to 100 million square-foot area"—"as much as 12,500 times less accurate than * * * GPS data." Pet. App. 14a-15a. The government ultimately determined that petitioner's phone connected to cell towers in the general vicinity of the sites of four robberies around the times those robberies occurred. *Id.* at 6a.

b. Petitioner was indicted on six Hobbs Act counts and six firearms counts. Pet. App. 4a. Before trial, petitioner moved to suppress the cell-site records. *Id.* at 7a-8a. Petitioner argued that MetroPCS's and Sprint's production of their business records constituted a Fourth Amendment search of petitioner that could be

conducted only pursuant to a warrant supported by probable cause. *Ibid.*

The district court denied the motion to suppress. Pet. App. 34a-48a. The court found "no legitimate expectation of privacy in cell site data," *id.* at 38a, and further held that suppression would not be an appropriate remedy even if a warrant were required "because the agents relied in good faith on the [SCA] in obtaining the evidence," *id.* at 38a n.1.

c. The case proceeded to trial, where seven accomplices testified about petitioner's involvement in the robberies. Pet. App. 5a. The government also introduced videotapes and eyewitness testimony placing petitioner near the relevant robbery scenes. See Gov't C.A. Br. 45-47 (describing evidence).

In addition, FBI Special Agent Christopher Hess offered expert testimony about the cell-site data for petitioner's phone. Pet. App. 5a-6a; J.A. 36-129. Agent Hess explained that petitioner's providers recorded tower information only when the phone was "active," meaning "[e]ngaging in a call." J.A. 60; see J.A. 61 (testimony that "if you dial a number and you hit send, that tower information is populated in the call detail record," but records are not created when "the phone is just in [a] pocket" and not making or receiving calls). "The parties stipulate[d] and agree[d] that the telephone call detail records from * * * Metro PCS and Sprint" were "authentic and accurate business records of these companies." J.A. 51; see J.A. 136 (cell-site record for petitioner's phone on December 13, 2010).[2]

---

[2] This document is the only cell-site record for petitioner's phone in the record. Amici asked the court of appeals to take judicial notice of all the cell-site records MetroPCS produced, but the court declined, stating that it would not "create an evidentiary loophole

Based on those records, Agent Hess identified eight calls that occurred around the time of four robberies. Pet. App. 80a-82a; J.A. 56-67, 77-79. He presented maps of the towers that connected those calls to demonstrate that petitioner's phone was within a half-mile to two miles of the crime scenes. Pet. App. 6a, 86a-89a. But Agent Hess could not offer "any opinion about exactly where a phone was at any particular time" within each tower's coverage area. J.A. 88. He acknowledged that he could not determine from the cell-site records whether petitioner's phone was at a specific parking lot or intersection, J.A. 86-87; whether the phone was north or south of a store, J.A. 95; whether the phone had connected to a particular tower based on proximity or other "variables, such as * * * the battery strength," J.A. 84; "who was actually using the phone at the time that the call was made," J.A. 88; or why the phone was located within a particular tower's coverage area at a particular time, J.A. 95-96. Agent Hess acknowledged that his analysis of cell-site records was "not an exact science." J.A. 97-98.

The jury convicted petitioner on all the Hobbs Act counts and all but one of the firearms counts. Pet. App. 6a. The district court sentenced petitioner to 1395 months in prison. *Id.* at 7a.

3. The court of appeals affirmed. Pet. App. 1a-32a.

a. As relevant here, the court of appeals rejected petitioner's Fourth Amendment challenge, holding that

---

through which a litigant could present a district court with one record and then ask an appellate court to reverse the district court based on another record." Order 2 (Apr. 11, 2016).

the government's acquisition of the cell-site records was not a search of petitioner. Pet. App. 8a-17a.

The court of appeals emphasized that petitioner "lack[s] any property interest in cell-site records created and maintained by [his] wireless carriers." Pet. App. 12a. As the court explained, MetroPCS and Sprint gathered information about which of their towers connected petitioner's calls "in the ordinary course of business" for their own purposes, such as "to find weak spots in their network and to determine whether roaming charges apply." *Id.* at 10a.

The court of appeals further concluded that petitioner had no reasonable expectation of privacy in those business records. Pet. App. 7a-13a. The court relied on *Smith* v. *Maryland*, 442 U.S. 735 (1979), which "held that the police's installation of a pen register—a device that tracked the phone numbers a person dialed from his home phone—was not a search because the caller could not reasonably expect those numbers to remain private." Pet. App. 9a-10a. Because "Smith 'voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business,'" the "numerical information was not protected under the Fourth Amendment." *Id.* at 12a (internal quotation marks omitted) (quoting *Smith*, 442 U.S. at 744). The court of appeals concluded that the same reasoning applied to cell-site records because cell-phone users voluntarily convey information to their providers about their phones' proximity to particular towers "as a means of establishing communication" when they place or receive calls. *Ibid.* (quoting *Smith*, 442 U.S. at 741).

The court of appeals observed that "[w]hether a defendant ha[s] a legitimate expectation of privacy in certain information depends in part on what the government did to get it." Pet. App. 13a. Because "[t]his case involves business records obtained from a third party," the court found any expectation of privacy to be "diminish[ed]." *Id.* at 14a. The court further emphasized that the cell-site location data was "as much as 12,500 times less accurate" than GPS data and contained only "routing information" that "sa[id] nothing about the content of any calls." *Id.* at 10a, 14a.

The court of appeals noted that, in enacting the SCA, Congress "struck a balance" by requiring the government to "show 'reasonable grounds' but not 'probable cause' to obtain" cell-site records. Pet. App. 15a-16a (citation omitted). The court observed that "Congress is usually better equipped than courts are to answer the empirical questions that [new] technologies present." *Id.* at 17a. The court concluded that "[t]hese concerns favor leaving undisturbed the Congressional judgment" reflected by the SCA's "middle ground [approach] between full Fourth Amendment protection and no protection at all." *Id.* at 15a, 17a.[3]

b. Judge Stranch filed an opinion concurring in the judgment on the Fourth Amendment issue. Pet. App. 24a-32a. In her view, the government's acquisition of the historical cell-site records "raise[d] Fourth Amendment concerns," but the district court properly denied

---

[3] Because the court of appeals concluded that no search had occurred, it did not reach the government's alternative arguments that (i) any search was constitutionally reasonable, see Gov't C.A. Br. 37-40; (ii) the good-faith exception to the exclusionary rule applies, see *id.* at 40-42; and (iii) any error in admitting the cell-site data was harmless, see *id.* at 44-47.

the motion to suppress under the good-faith exception to the exclusionary rule. *Id.* at 24a-25a.

SUMMARY OF ARGUMENT

I. The government's acquisition of cell-site records from MetroPCS and Sprint did not constitute a Fourth Amendment search of petitioner.

A. Petitioner has no legitimate expectation of privacy in the business records his providers made of the cell towers used to route calls to and from his cell phone. This Court has long held that an individual cannot invoke the Fourth Amendment to object to the government's acquisition of a third party's records that contain information about the individual. See *Smith* v. *Maryland*, 442 U.S. 735 (1979) (records of dialed calls); *United States* v. *Miller*, 425 U.S. 435 (1976) (banking records).

The third-party doctrine applies here. Petitioner had no subjective expectation of privacy in his providers' records of the towers used to connect his calls. Cell-phone users are aware that they must be in a tower's coverage area to use their phones, and they must understand that their provider knows the location of its own equipment and may make records of the use of its towers. And any subjective expectation of privacy would not be objectively reasonable. Cell-phone users voluntarily reveal to their providers information about their proximity to cell towers so the providers can connect their calls. Users cannot reasonably expect that the providers will not reveal that business information to the government.

Contrary to petitioner's suggestion, cell-site records are not more sensitive than the records of phone numbers dialed and banking records at issue in *Smith* and *Miller*. Inferences about location drawn from cell-site

information are far less precise than GPS data and do not permit a detailed reconstruction of a person's movements. And in any event, the third-party doctrine does not turn on *what* information the government acquires and how sensitive that information is, but rather on *how* the government acquires the information. Seeking information about a suspect from a third-party witness does not amount to a Fourth Amendment search of that suspect, no matter how revealing or incriminating the evidence may be. Nor was petitioner's action in conveying information about his proximity to cell towers less "voluntary" than the defendants' actions in *Smith* and *Miller*. In those cases, like this one, individuals were required to reveal information about themselves to use an important service provided by a business that was a ubiquitous part of modern society.

Cell-service providers' use of technology does not justify a new Fourth Amendment rule. This case involves a traditional procedure used for centuries: compulsory process to a third party. The relevant change is not in government conduct, but in the actions of private providers in creating cell-tower networks and recording information about the networks' use. But a private actor's decision to acquire and record information is not a subject of Fourth Amendment protection.

Petitioner suggests that if the third-party doctrine is applied here, it would permit unregulated government collection of all information in a third party's hands, including email. That is incorrect. Email is routed through a provider, and its contents, like those of a sealed letter in the mail, may remain private. But cell-tower information is sent to the provider and used in its own business; it falls within the traditional third-party

doctrine. Moreover, adherence to the third-party doctrine does not eliminate all constitutional limitations on collection of data. Providers may invoke their own Fourth Amendment rights to object to compulsory process that exceeds legislative authorization, sweeps too broadly, or imposes undue burdens. The sensitivity of customer information may inform that calculus. The First Amendment and equal protection principles also protect against abuses. And if businesses' possession of great quantities of digital information raises new privacy concerns, legislatures are well positioned to address them.

B. Petitioner was not subject to a trespassory search under *United States* v. *Jones*, 565 U.S. 400 (2012). He can establish no protected interest in the providers' cell-tower records, and his reliance on positive law to claim such an interest lacks merit.

II. If the government's acquisition of cell-site records amounted to a search of petitioner, it was constitutionally reasonable.

A. Under longstanding Fourth Amendment principles, the government's use of compulsory process to obtain records does not require a warrant. Section 2703(d) falls within that tradition and in fact raises the bar from a subpoena by requiring a specific factual showing and a court order, thereby adequately protecting any expectation of privacy a customer could assert in cell-site records.

B. Applying standard Fourth Amendment balancing principles leads to the same conclusion. Any privacy interest in third-party business records is diminished. And the government has a compelling interest in obtaining cell-site records to identify suspects, clear the inno-

cent, and obtain information in the preliminary investigation of criminal conduct. Deference to Congress's judgment in Section 2703(d) is appropriate in this new technological context.

III. If the Court concludes that a warrant is required to obtain some cell-site records, it should hold, as petitioner concedes, that requests for short-term cell-site records fall outside that rule. Here, that principle would validate the request for seven days of records from Sprint, as that is well within the range of ordinary visual surveillance of a person suspected of a crime.

ARGUMENT

I. THE GOVERNMENT'S ACQUISITION OF PROVIDERS' BUSINESS RECORDS OF THE TOWERS USED TO CONNECT PETITIONER'S CALLS DID NOT CONSTITUTE A FOURTH AMENDMENT SEARCH OF PETITIONER

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. An individual may claim protection against a Fourth Amendment "search" in two circumstances. First, he may establish that he has been searched if "the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo* v. *United States*, 533 U.S. 27, 33 (2001); see *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Second, he may establish that he has been searched if he is subject to a "physical intrusion of a constitutionally protected area," in a manner that would constitute a "common-law trespass." *United States* v. *Jones*, 565 U.S. 400, 405, 407 (2012) (citation omitted). Under either approach, the government's acquisition of

MetroPCS's and Sprint's business records of the cell towers used to connect petitioner's calls did not constitute a Fourth Amendment search of petitioner.

A. A Cell-Phone User Has No Reasonable Expectation Of Privacy In Business Records Created By His Provider Documenting The Cell Sites Used To Connect His Calls

1. Petitioner cannot claim a legitimate privacy interest in information about his proximity to cell towers that he disclosed to his cell-service providers

a. "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith* v. *Maryland*, 442 U.S. 735, 743-744 (1979). Third-party service providers who receive such information are free to create business records pertaining to the service they provide to their customers. *Id.* at 745. And the Court has held that the government's subsequent acquisition of those records does not constitute a Fourth Amendment search of the customer. See *id.* at 744-745; *United States* v. *Miller*, 425 U.S. 435, 442-443 (1976).

In *Miller*, the government subpoenaed a defendant's banks for several months of records of his accounts, including copies of his checks, deposit slips, financial statements, and monthly statements. 425 U.S. at 436-438. The defendant contended that he had "a reasonable expectation of privacy" in those records because "they [were] merely copies of personal records that were made available to the banks for a limited purpose." *Id.* at 442. But the Court rejected that argument, observing that it had "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him

to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose." *Id.* at 443. The Court explained that the defendant could "assert neither ownership nor possession" of the records; rather, they were "business records of the banks." *Id.* at 440. Because those records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," the Court concluded that the defendant had "take[n] the risk, in revealing his affairs to another, that the information w[ould] be conveyed by that person to the Government." *Id.* at 442, 443.

In *Smith*, the Court applied the same principles to information conveyed to a telephone company. There, the police requested that the defendant's telephone company install a pen register at its offices to record the numbers dialed from the defendant's home phone. 442 U.S. at 737. The Court rejected the defendant's argument that the government's acquisition of the records of his dialed numbers qualified as a Fourth Amendment search. *Id.* at 742-746.

Smith first expressed "doubt that people in general entertain any actual expectation of privacy in the numbers they dial," given 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. The Court believed that the typical user would be aware that the phone company could choose to record the numbers he dialed and would "in fact record this information for a variety of legitimate business purposes." *Id.* at 743. "Most phone books," the Court observed, inform users "that the [phone] company can frequently help in identifying to the authorities the origin

of unwelcome and troublesome calls." *Id.* at 742-743 (internal quotation marks omitted).

Smith went on to explain that "even if [the defendant] 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." 442 U.S. at 743 (citation and internal quotation marks omitted). "When [the defendant] used his phone," the Court observed, he "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business." *Id.* at 744 (internal quotation marks omitted). Because the company was "free to record" the information the defendant conveyed about the numbers he was dialing, the Court concluded that he "assumed the risk" that the company's records "would be divulged to police." *Id.* at 745.

The Court's recognition that individuals cannot claim a reasonable expectation of privacy vis-à-vis the government in information they disclose to third parties has deep historical roots. It is an "ancient proposition of law" that "'the public . . . has a right to every man's evidence,' except for those persons protected by a constitutional, common-law, or statutory privilege." *United States* v. *Nixon*, 418 U.S. 683, 709 (1974) (citation omitted). "[A]s early as 1612, * * * Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.'" *Blair* v. *United States*, 250 U.S. 273, 279-280 (1919) (quoting *Countess of Shrewsbury Case*, 2 How. St. Tr. 769, 778 (1612)). As this Court has recognized, "[t]o ensure that justice is done, it is imperative to the function of courts that compulsory process be

available for the production of evidence." *Nixon*, 418 U.S. at 709.

A witness who observes relevant events must therefore testify about them when asked to do so, unless a recognized privilege applies. A desire for privacy does not trigger a privilege, as no "constitutional provision protects the average citizen from disclosing * * * information that he has received in confidence." *Branzburg* v. *Hayes*, 408 U.S. 665, 682 (1972). Accordingly, a person who "rel[ies] upon his misplaced confidence that [a third party] w[ill] not reveal his wrongdoing" cannot claim a legitimate expectation that the information will remain private. *Hoffa* v. *United States*, 385 U.S. 293, 302 (1966). He therefore cannot invoke the Fourth Amendment to prevent the government from obtaining the third party's testimony, evidence, or records that reveal matters he has disclosed. *SEC* v. *Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984).

b. The Court's third-party cases establish that petitioner has no Fourth Amendment interest in MetroPCS's and Sprint's records of the cell towers they used to connect his calls.

i. Petitioner lacks any subjective expectation of privacy in the cell-site information because his providers compiled that data based on their transactions with petitioner for their own business purposes. See Pet. App. 7a, 10a. As with the bank records in *Miller*, petitioner "can assert neither ownership nor possession" of the cell-site records, 425 U.S. at 440; indeed, he "stipulate[d] and agree[d]" that they were "business records of [MetroPCS and Sprint]." J.A. 51. "Although subjective expectations cannot be scientifically gauged," cellphone users, like landline users, should not be pre-

sumed to have a "general expectation" that data generated by their use of telephone-company equipment and incorporated into the company's records "will remain secret." *Smith*, 442 U.S. at 743.

Petitioner contends (Br. 42-44) that cell-phone users may not realize the extent of the information they disclose about their location when they use their providers' towers to connect their calls. But as petitioner recognizes (Br. 42-43), cell-phone users surely "have a general sense that their cell phones must communicate with the service provider's cell towers in order to place and receive calls." "[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower." Pet. App. 12a; see, *e.g.*, *United States* v. *Graham*, 824 F.3d 421, 430 (4th Cir. 2016) (en banc), petitions for cert. pending, Nos. 16-6308 and 16-6694 (filed Sept. 26 and Oct. 27, 2016); *United States* v. *Davis*, 785 F.3d 498, 511 (11th Cir.) (en banc), cert. denied, 136 S. Ct. 479 (2015); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013) (*Fifth Circuit In re Application*); see also *Smith*, 442 U.S. at 743 (relying on what telephone users "typically know" to refute any subjective expectation of privacy). If any doubt existed on that point, "contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls." *Fifth Circuit In re Application*, 724 F.3d at 613; see p. 3 n.1, *supra* (citing policies); see also *Smith*, 442 U.S. at 742-743 (finding no subjective privacy expectation in dialed numbers in part because "[m]ost phone

books t[old] subscribers" that the phone company could help identify the source of unwelcome calls).[4]

Petitioner further errs in asserting (Br. 43) that cell-phone users may subjectively expect that routing information for their calls will remain private because they "do not receive their [cell-site location information] in their monthly bill" and "cannot know whether the service provider is logging and retaining that data and in what form or detail." The *Smith* Court rejected similar arguments. There, the Court acknowledged that "most people may be oblivious to a pen register's esoteric functions," 442 U.S. at 742, and that telephone users would not ordinarily see lists of the local numbers they dialed because "telephone companies, in view of their present billing practices, usually do not record local calls," *id.* at 745. But the Court nevertheless found that users are generally aware that companies can track the numbers dialed and are "free to record" that information. *Ibid.* Cell-phone users similarly should be charged with knowledge "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 con-

---

[4] Petitioner notes (Br. 42) that some smart phones "have a location privacy setting that, when enabled, prevents applications" from using GPS data to access a phone's location. Petitioner speculates that users who enable that feature may incorrectly think they are preventing their providers from collecting cell-site data. Any such misconception contradicts the providers' privacy policies and users' understanding that their phones must connect to cell towers to work. And if a cell-phone user elected *not* to enable the privacy setting, that conduct would simply confirm that the user lacked a subjective expectation of privacy in the data her provider collects.

veying 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" or are free to do so. *Davis*, 785 F.3d at 511.

ii. In any event, any subjective expectation of privacy in information a user conveys to his provider about his proximity to cell towers would not be objectively reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-744. Just as a person who dials a phone number "voluntarily convey[s] numerical information to the telephone company and expose[s] that information to its equipment in the ordinary course of business," *id.* at 744 (internal quotation marks omitted), a cell-phone user reveals general information about his location to his provider so that it can connect his calls. A cell-phone user thus has no valid basis for complaint if the provider makes use of that business information, including by providing it to the government. See *Miller*, 425 U.S. at 443.

Petitioner contends (Br. 21) that his asserted expectation of privacy is reasonable based on "protections adopted in federal and state law." Petitioner relies (Br. 21-22) on 47 U.S.C. 222, which generally prohibits cell-service providers from using or disclosing certain information, including cell-site information and records of the numbers a customer has dialed. 47 U.S.C. 222(c)(1), (d), and (h)(1). But the statute enumerates several exceptions to that general rule and further permits disclosure "as required by law," 47 U.S.C. 222(c)(1)—which includes a valid court order

issued pursuant to the SCA.[5] A cell-phone user consulting federal law therefore could not reasonably believe that Section 222 prevents the government from obtaining providers' cell-site records. Nor could this Court credit such a belief without overruling *Smith*'s holding that users have no reasonable expectation of privacy in the phone numbers they dial—a category of information also protected by Section 222. See 47 U.S.C. 222(h)(1).

Petitioner's reliance on Section 222 is also wrong as a matter of Fourth Amendment jurisprudence. Although statutes "enacted in the years immediately before or after the [Fourth] Amendment was adopted shed light on what citizens at the time of the Amendment's enactment saw as reasonable," the Court has rejected the suggestion that "the Amendment was intended to incorporate subsequently enacted statutes." *Virginia* v. *Moore*, 553 U.S. 164, 169 & n.3 (2008). Congress can enact statutory privacy protections that go beyond the Fourth Amendment floor—and it has restricted disclosure of a variety of third-party records pertaining to individuals who cannot claim Fourth Amendment protection of those records. See, *e.g.*, 15 U.S.C. 6802 (financial records); 26 U.S.C. 7216 (information used to prepare tax returns). But "no historical indication [exists] that those who ratified the Fourth Amendment understood it as a redundant guarantee of" statutory protections. *Moore*, 553 U.S. at 168.

---

[5] Petitioner notes (Br. 22) that Section 222 requires providers to obtain a user's "express prior authorization" before disclosing location data based on the user's consent. 47 U.S.C. 222(f). But that rule for establishing consent does not displace the many other provisions permitting disclosure *without* the user's approval, including "as required by law." 47 U.S.C. 222(c)(1).

Petitioner's reliance on state law (Br. 22-23) is similarly misplaced. Some States have required a search warrant for historical cell-site records as a matter of state law, but this Court has repeatedly rejected the "suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment." *California* v. *Greenwood*, 486 U.S. 35, 44 (1988). Rather, "when States go above the Fourth Amendment minimum, the Constitution's protections concerning search and seizure remain the same." *Moore*, 553 U.S. at 173. The enactment of state laws addressing cell-site records confirms that legislatures are best positioned to balance privacy interests and law-enforcement needs in light of new technologies, as Congress did in the SCA. See *Jones*, 565 U.S. at 429-430 (Alito, J., concurring in the judgment). But state laws do "not alter the content of the Fourth Amendment" and so cannot help petitioner establish that the government's acquisition of his cell-service providers' business records constituted a Fourth Amendment search of him. *Moore*, 553 U.S. at 172.

2. Petitioner cannot distinguish this Court's cases finding no reasonable expectation of privacy in information conveyed to a third party

Petitioner argues (Br. 35-47) that the third-party doctrine should not apply to longer-term cell-site records, but his attempts to distinguish *Smith* and *Miller* lack merit.

a. Petitioner asserts (Br. 36) that "[t]he particular records at issue here are far more sensitive and personal than those in *Smith* and *Miller*." That contention is both factually inaccurate and legally irrelevant.

i. Petitioner stakes his asserted expectation of privacy on his claim (Br. 3) that the government's acquisition of cell-site information "make[s] it possible to reconstruct in detail everywhere an individual has traveled over hours, days, weeks, or months." That is incorrect. Although petitioner likens cell-site records to GPS tracking, cell-site location information is actually "as much as 12,500 times less accurate" than GPS data. Pet. App. 14a. Rather than pinpoint petitioner's precise location, the records identified "a 3.5 million square-foot to 100 million square-foot area," *ibid.*—an area that would cover about 180 to 5155 oval plazas equal in size to the one in front of the Supreme Court building. See *Hodge* v. *Talkin*, 799 F.3d 1145, 1151 (D.C. Cir. 2015) (providing measurements of the Court's plaza), cert. denied, 136 S. Ct. 2009 (2016). When such an area encompasses a crime scene, cell-site records may be consistent with the government's theory that a defendant was there, but they do not on their own suffice to place him at the crime scene. See Pet. App. 89a. The government must instead rely on reasonable inferences or additional evidence—*e.g.*, eyewitness accounts and video surveillance like that introduced at petitioner's trial—to develop proof of a defendant's movements.

The cell-site records in this case illustrate the point. On December 13, 2010, for example, petitioner's phone connected to two cell towers close in time to the robbery of a Radio Shack in Detroit. Pet. App. 86a. During the first call, petitioner's phone connected to a tower more than a dozen blocks southwest of the Radio Shack, and during the second call, petitioner's phone initially connected to a tower at least eight blocks northeast of the store. *Ibid.* An excerpt of the map Agent Hess created shows that area:

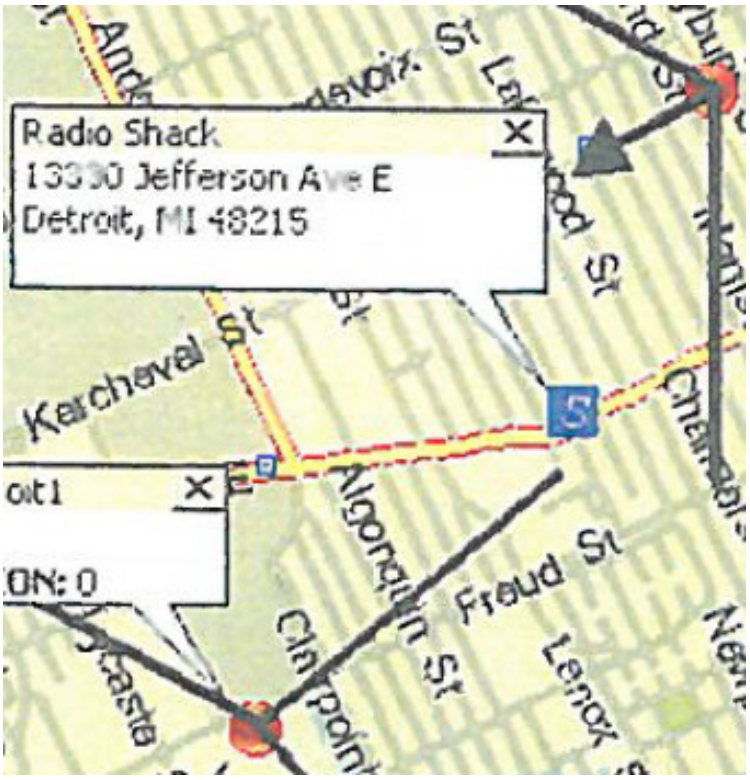

Figure 1 – Excerpt from Gov't Ex. 57 (Pet. App. 86a)

As reflected in the following illustration using data from Google Maps, the area approximately within the relevant tower sectors today contains about 1000 buildings, including hundreds of homes, various commercial establishments, more than one dozen houses of worship, several civic buildings, numerous multi-unit apartment buildings, and a large automobile assembly plant.[6]

---

[6] Appendix B, *infra*, 13a, explains the methodology used to create Figure 2, which is not in the record and is offered to illustrate the approximate density and variety of buildings in the area given petitioner's assertion (Br. 17) that cell-site records reveal religious preferences, doctor's visits, shopping habits, or other places visited.

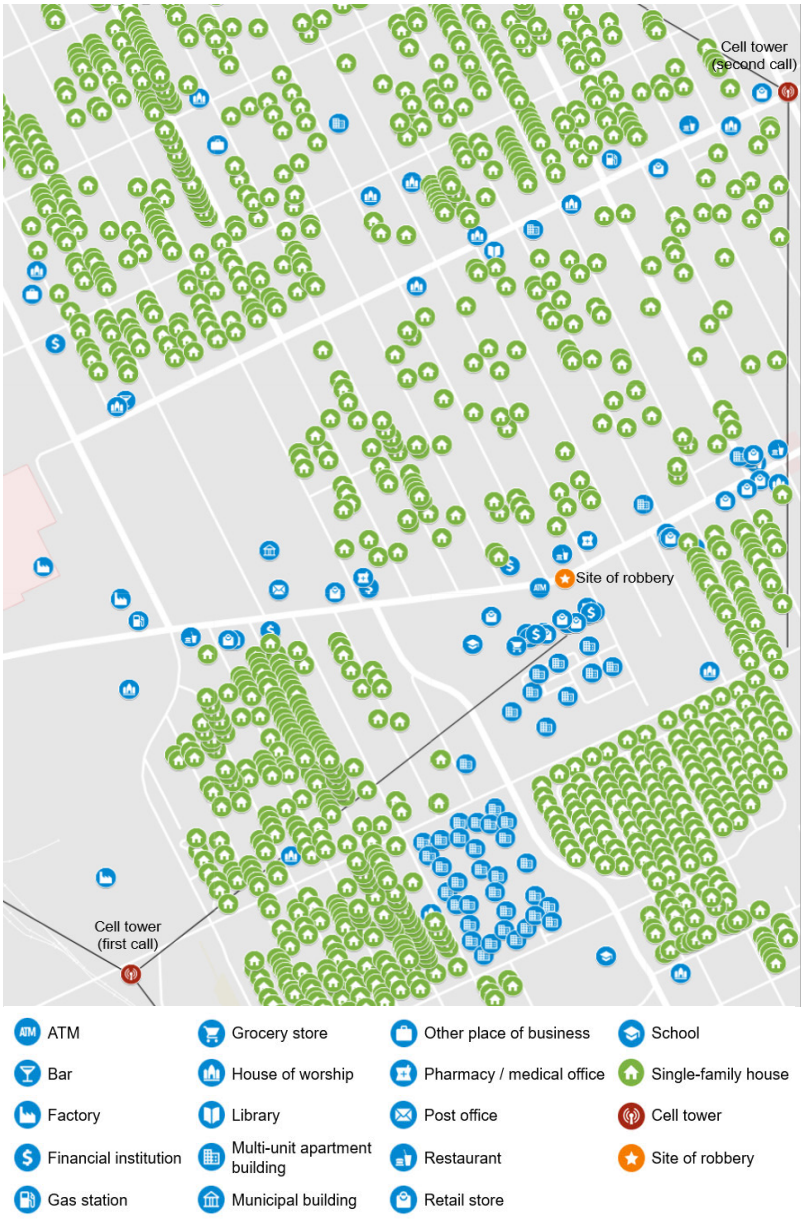

Figure 2 – Illustrative map of buildings in the area

While the cell-site data corroborated other evidence of petitioner's participation in the December 13 robbery, it could not reveal the exact whereabouts of his phone within the towers' coverage area. J.A. 88, 131-132. From the records alone, the government could not determine whether petitioner (or someone using his phone) was at the Radio Shack, or instead at any one of the nearby bars, restaurants, stores, schools, banks, gas stations, other commercial establishments, or homes.

Petitioner contends (Br. 27-29) that cell-site records will enable more precise inferences about an individual's location in the future as providers deploy cell towers with smaller coverage areas. But petitioner identifies no case in which the government has obtained records involving small-cell technology. And the technology could develop in a different direction. For example, device-to-device technology could reduce the need for cell towers, preventing providers from collecting or recording location information. See, *e.g.*, Tom Simonite, *Future Smartphones Won't Need Cell Towers to Connect*, MIT Tech. Review, Sept. 29, 2014, https://www.technologyreview.com/s/530996/future-smartphones-wont-need-cell-towers-to-connect/ (describing technology); Qualcomm, *LTE Direct Proximity Services*, https://www.qualcomm.com/invention/technologies/lte/direct (last visited Sept. 25, 2017) (asserting that device-to-device technology protects location privacy because it "allow[s] the devices to discover others without revealing their own identity or exact location"). Similarly, all major cell-service providers now offer built-in wi-fi calling, which may reduce providers' access to "network location information." Lennart Norell et al., *Wi-Fi calling —extending the reach of VoLTE to Wi-Fi*, Ericsson Review 1, 3-5 (Jan. 30, 2015), https://www.ericsson.com/

res/thecompany/docs/publications/ericsson_review/2015/er-wifi-calling.pdf. Because the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear," it should decline petitioner's invitation to consider the Fourth Amendment's application in hypothetical circumstances not presented by the facts of his case. *City of Ontario* v. *Quon*, 560 U.S. 746, 759 (2010).

ii. In any event, petitioner errs in suggesting that the sensitivity of information in a third party's records triggers a reasonable expectation of privacy in those records.[7] The application of the third-party doctrine does not depend on the quantity of information disclosed to the third party or on how revealing or incriminating that information may be. Records of the telephone numbers a person dials may reveal intensely personal information about her associations. See *Smith*, 442 U.S. at 748 (Stewart, J., dissenting) (observing that such records "easily could reveal the identities of the persons and the places called, and thus

---

[7] Petitioner cites (Br. 37) *Ferguson* v. *City of Charleston*, 532 U.S. 67 (2001), and *Stoner* v. *California*, 376 U.S. 483 (1964), but those cases did not address whether the government conducts a search of an individual by acquiring information about him that he has conveyed to a third party. *Ferguson* involved urine tests that "were indisputably [Fourth Amendment] searches," 532 U.S. at 76, and the only question was whether "special needs" allowed government actors to conduct the tests and share the results with nonmedical personnel, *id.* at 77-81. *Stoner* involved a Fourth Amendment search of a hotel room, and the only question was whether the clerk who unlocked the door for the officers had authority to consent to the search. 376 U.S. at 485-488.

reveal the most intimate details of a person's life").[8] Records detailing every banking transaction an individual conducts likewise may contain sensitive information about her finances, spending habits, and financial relationships. *Miller*, 425 U.S. at 451 (Brennan, J., dissenting) (observing that "the totality of bank records provides a virtual current biography" because "[i]n the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations") (citation omitted). Despite the sensitivity of that information, this Court has recognized that disclosure to a third party vitiates a reasonable expectation that the information will remain private, "even if [it] 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 (majority opinion). Accepting petitioner's argument about sensitive third-party records would not provide a way to distinguish *Smith* and *Miller*, but would instead represent a stark departure from their rationales.

Petitioner's contention (Br. 37-38) that "the 'third party' doctrine * * * can be overcome when highly sensitive information is at stake" would also generate intractable line-drawing problems. Petitioner suggests no framework for determining when information conveyed to a third party should be considered sufficiently

---

[8] Empirical studies have established that "a similar number of adults regard the phone numbers they call to be just as 'sensitive' as location data." *United States* v. *Graham*, 796 F.3d 332, 382 n.5 (4th Cir. 2015) (Motz, J., dissenting in part and concurring in the judgment) (citing Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era* 34-35 (Nov. 12 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf), rev'd en banc, 824 F.3d 421 (4th Cir. 2016).

sensitive that it gives rise to a Fourth Amendment interest. And investigators cannot reasonably apply the standard to determine which third-party record requests require a warrant because they cannot know the particular contents of the records or the quantity of information they contain in advance. See *Atwater* v. *City of Lago Vista*, 532 U.S. 318, 347 (2001) (observing that "a responsible Fourth Amendment balance is not well served by standards requiring sensitive, case-by-case determinations * * * lest every discretionary judgment in the field be converted into an occasion for constitutional review").

Petitioner's proposed revision of the third-party doctrine is unworkable even as applied to location information. Petitioner concedes (Br. 29-31) that individuals have no reasonable expectation of privacy in records that reveal some amount of location data. But he declines to suggest how much is too much. And it is not evident when his rule would bar investigators from accessing a variety of records that may reveal information about a person's location or movements—from credit-card records that identify the places and times he made purchases, to IP-address records that reveal when he used a computer in a particular location, to pen-register records that show when he made calls from his home telephone, to key-card-entry records that reflect his regular hours at a gym. The practical problems posed by petitioner's argument counsel against his innovative suggestion that individuals may claim a Fourth Amendment interest in the records of their transactions with businesses from which their location can be inferred.

b. Petitioner further seeks to distinguish *Miller* and *Smith* (Br. 39-44) by contending that cell-phone users

do not voluntarily convey information about their location to their providers. Petitioner emphasizes (Br. 39) the importance of cell-phone use in modern society and argues that "[t]he act of possessing a cell phone, and even more so the transmission of location information, is not voluntary in any meaningful way."

Petitioner's argument misunderstands the circumstances under which this Court has applied the third-party doctrine. An individual who shares information about himself in the course of obtaining a third party's services need not necessarily be happy to expose those private details of his life to the business. Indeed, he may feel as though he has no choice if he wishes to use the third party's services. The depositor in *Miller*, for example, may not have relished sharing his financial affairs with his bank, as necessary to conduct banking transactions. See 425 U.S. at 451 (Brennan, J., dissenting) (observing that the depositor's actions were "not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account"). The telephone user in *Smith* likewise had no choice but to communicate the numbers he dialed to his telephone company, unless he was "prepared to forgo use of what for many has become a personal or professional necessity." 442 U.S. at 750 (Marshall, J., dissenting). But this Court nevertheless found that the individuals in *Smith* and *Miller* had "voluntarily conveyed" information about themselves to third parties—even though they had no ability to avoid exposing the information short of discontinuing use of the third party's services. *Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 442.

Petitioner accordingly cannot avoid application of the third-party doctrine by observing (Br. 39) that cell

phones are "a pervasive and insistent part of daily life." *Riley* v. *California*, 134 S. Ct. 2473, 2484 (2014). An individual's decision to expose his proximity to cell towers to his cell-service provider so it can connect his calls is just as volitional as his action in exposing the numbers he dials to that provider for the same purpose—and petitioner accordingly has not offered a tenable way to distinguish *Smith* and *Miller*.

3. Cell-service providers' use of technology supplies no basis to depart from well-established Fourth Amendment principles

Petitioner contends (Br. 10-11) that the Court should exempt cell-site records from the third-party doctrine because cell-service providers used technology to collect "a great volume" of information about him that the government could not have obtained "prior to the digital age." The Court should reject that argument.

1. In analyzing whether a Fourth Amendment search has occurred "it is important to begin by specifying precisely the nature of the state activity that is challenged." *Smith*, 442 U.S. at 741; see *Jones*, 565 U.S. at 404 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information."). This Court's focus on the character of the government's conduct reflects that the existence of a Fourth Amendment search turns on *how*—not just *whether*—information is obtained. For example, "[a] phone conversation is private when overheard by means of a wiretap; but that same conversation is unprotected if an agent is forced to overhear it while seated on a Delta flight." Pet. App. 13a. "Similarly, information that is not particularly sensitive—say, the color of a suspect's vehicle—might be protected if government

agents broke into the suspect's garage to get it," but "information that is highly sensitive—say, all of a suspect's credit-charges over a three-month period—is not protected if the government gets that information through business records obtained per a subpoena." *Ibid.*

The government here obtained a third party's business records pursuant to a court order authorized by law. The character of the government's conduct fundamentally distinguishes this case from those in which the Court has expressed concern about the potential of new technology to erode privacy. Petitioner cites (Br. 15) *Jones*, *supra*, and *Kyllo*, *supra*, but in those cases government agents used technology to enhance their surveillance of a suspect.[9] In *Jones*, the government surreptitiously installed a GPS tracking device on a vehicle to monitor its movements for 28 days. 565 U.S. at 402-403. And in *Kyllo*, the government used a thermal imaging device that was "not in general public use[] to explore details of the home that would previously have been unknowable without physical intrusion." 533 U.S. at 40. In both cases, this Court held that the

---

[9] Petitioner also cites (Br. 15) *Riley*, *supra*, which held that officers generally must obtain a warrant before "search[ing] digital information on a cell phone seized from" an arrestee. 134 S. Ct. at 2480. But the government action in *Riley* indisputably constituted a Fourth Amendment search, and the only question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. See *id.* at 2482. The analysis in *Riley* sheds no light on whether the qualitatively different government action of seeking evidence from a third party is a search in the first place. See *id.* at 2489 n.1 (explaining that the case did "not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances").

government's conduct constituted a search—a result that the Court concluded would "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Jones*, 565 U.S. at 406 (brackets in original) (quoting *Kyllo*, 533 U.S. at 34). But the Court's analysis in both cases made clear that the Fourth Amendment protects against particular *means* of acquiring information—not against the end results of that action. See *id.* at 408 n.5 ("[T]he obtaining of information is not alone a search unless it is achieved by * * * a trespass or invasion of privacy."); *Kyllo*, 533 U.S. at 35 n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment.").

Far from "employ[ing] new technology" in this case, Pet. Br. 10, the government used a method of obtaining evidence that was in use at least two hundred years before adoption of the Fourth Amendment: compulsory process to witnesses. See *Blair*, 250 U.S. at 279-280 (describing history of compulsory process dating to 1562). "[T]he general common-law principle that 'the public has a right to every man's evidence' was considered an 'indubitable certainty' that 'c[ould not] be denied' by 1742." *Kastigar* v. *United States*, 406 U.S. 441, 443 (1972). "[G]uidance from the founding era," *Riley*, 134 S. Ct. at 2484, therefore confirms that the government's conduct in seeking information about an individual from a third party has never been understood to constitute a Fourth Amendment search of that individual.

2. Petitioner's technology-based argument accordingly must focus on the actions of his *cell-service providers* in collecting and recording information about which towers they used to connect his calls. Even if that

conduct intruded on petitioner's privacy interests, however, the Fourth Amendment does not protect him from that private action. See *United States* v. *Jacobsen*, 466 U.S. 109, 113 (1984) (Fourth Amendment "proscrib[es] only governmental action"). And the government's later acquisition of the providers' business records likewise cannot be characterized as a Fourth Amendment search of petitioner because the government did not "exceed[] the scope" of any intrusion by the providers. *Id.* at 115.

The Court applied those principles to reject a Fourth Amendment challenge in *Jacobsen*. There, employees of a common carrier opened a damaged cardboard box and saw drugs inside. 466 U.S. at 111. They notified federal agents, who reopened the box and found the drugs. *Id.* at 111-112. This Court concluded that the agents' action "infringed no legitimate expectation of privacy and hence was not a 'search' within the meaning of the Fourth Amendment." *Id.* at 120. That result "follow[ed] from the analysis applicable when private parties reveal other kinds of private information to the authorities." *Id.* at 117 (citing, *inter alia*, *Miller*, 425 U.S. at 443, and *Smith*, 442 U.S. at 743-744). "Once frustration of the original expectation of privacy occurs" through a third party's action, the Court explained, "the Fourth Amendment does not prohibit governmental use of the now nonprivate information." *Ibid.* Accordingly, the "Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated." *Ibid.*

To the extent the cell-service providers intruded on petitioner's privacy interests by recording which towers they used to route his calls, the government played no

role in that conduct. Petitioner's providers created and maintained those cell-site records for their own business purposes. See Pet. App. 10a. They chose when to collect tower information and how long to retain those records. Indeed, the government has far less to do with the record collection here than in *Miller*, where federal law mandated that banks keep records of banking transactions. 425 U.S. at 443. Here, the cell-service providers not only decided what cell-site records to keep, but whether and when to use the data they collected for commercial purposes. See p. 3, *supra*. Because the government's acquisition of the providers' records did not reveal any information that the providers had not already themselves obtained, the Fourth Amendment does not protect against disclosure of the cell-site information.

3. Petitioner contends (Br. 44-47) that applying the third-party doctrine to cell-site records will permit unregulated government acquisition of all digital information in a third party's possession, including email content. That argument ignores the distinction between information conveyed to the provider and information conveyed to others that the provider merely carries, transports, or stores. Moreover, the government faces various limitations on its ability to collect data from third parties, and policymakers can enact additional privacy protections if society deems them warranted.

a. Application of the third-party doctrine here does not mean (Pet. Br. 45) that "people would have no reasonable expectation of privacy even in their emails, because the contents of those communications are shared with a third party." The Court has made clear that in-

dividuals who rely on a third party to deliver their communications do not thereby lose an expectation of privacy in the contents of those communications. See *Ex parte Jackson*, 96 U.S. 727, 733 (1878). Thus, a person who mails a private letter retains a legitimate expectation of privacy in its contents, even though the letter travels through the hands of postal carriers en route to its destination. *Ibid.* At the same time, no privacy expectation exists in the routing information conveyed to the carriers to facilitate the delivery. See *ibid.* The differential treatment of those categories of information turns on whether the information has been communicated *to* the providers or merely passes *through* their communications networks, with no general right of the provider to use or control the contents. From the providers' point of view, "the content of personal communications is private" but "the information necessary to get those communications from point A to point B is not." Pet. App. 9a.

Petitioner is therefore wrong to assert (Br. 47) that "there is no way to distinguish emails" from cell-site records. Cell-phone users do not convey the content of their emails, calls, and text messages to their cell-service providers for the providers' unrestricted use. But the users do convey information to their providers about the users' proximity to particular cell towers to enable the routing of those emails, calls, and text messages. Applying the third-party doctrine to business records that providers create from that routing information, which pertain to the customers' use of the providers' towers, accordingly would not undermine

Fourth Amendment protection for the content of those private communications.[10]

b. Petitioner states (Br. 46) that individuals today disclose a "vast array of information" about themselves to third parties when using those parties' services. See also *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring). Third parties' business records thus may contain increased quantities of information, as individuals choose to disclose that information to obtain desired services. But the character of the government's conduct—using compulsory process to obtain those records—has not changed. That conduct therefore is still not a Fourth Amendment search of the customer.

Petitioner expresses concern (Br. 14) that applying the third-party doctrine to records of his tower connections will leave all such data beyond constitutional control, making it possible for the government to collect all Americans' cell-site data for all time. That is incorrect. Providers have Fourth Amendment rights and may enforce well-established limits on the government's ability to request their business records, including protections

---

[10] Courts have recognized that the Fourth Amendment may protect the content of communications routed through a third-party provider even when the provider retains a limited right of access. See, *e.g.*, *United States* v. *Warshak*, 631 F.3d 266, 287 (6th Cir. 2010) (observing that "at the time *Katz* was decided, telephone companies had a right to monitor calls in certain situations"). Such incidental access does not undermine the principle that "the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected." *Fifth Circuit In re Application*, 724 F.3d at 611. Cell-site records, however, are not protected because they "are the providers' own records of transactions to which it is a party" and contain only information that is conveyed to providers so that they can route their customers' calls. *Id.* at 612.

against arbitrariness, overbreadth, and burdensomeness. See pp. 44-45, *infra*. That framework, enforceable through pre-compliance judicial review, can protect against "dragnet" collection efforts (Pet. Br. 45), even though individual customers cannot claim to have been searched. Cf. *United States* v. *Knotts*, 460 U.S. 276, 283-284 (1983) (reserving judgment on whether the Fourth Amendment may apply differently to "dragnet-type law enforcement practices"). The use of compulsory process also requires legislative authorization, see p. 44, *infra*, thus ensuring democratic accountability and legislative balancing of societal needs and individual interests, as appropriate for emerging technologies.

Limitations other than the Fourth Amendment also apply. The First Amendment regulates acquisition or use of information to suppress free speech or association, and equal protection principles protect against "intentionally discriminatory application of laws." *Whren* v. *United States*, 517 U.S. 806, 813 (1996). Those guarantees protect against abusive acquisition of cell-site records—just as with acquisition of banking records or pen-register records of numbers dialed.

Petitioner states (Br. 56-57) that investigators act unreasonably by requesting cell-site data spanning the weeks surrounding a crime. But collection of data before and after an unsolved crime is not arbitrary. Because cell-site records cannot identify an individual's exact location within a tower's coverage area, several weeks of data can help establish whether an individual's phone frequently connects to that tower—which could be "relevant" in determining whether the individual was at the crime scene or instead "had other reasons for being in that neighborhood." J.A. 128. Access to multiple weeks of data can also help officers confirm or refute

the possibility that the suspect frequently loans his phone to others, and did not possess it at the relevant time, thus exonerating the innocent. In any event, as with any demand for third-party records, courts can step in if law enforcement requests are excessive. See p. 45, *infra*.

Ultimately, if the quantity of information now available in third-party business records raises novel privacy concerns, the proper body to address them is the legislature. Members of this Court have recognized that "concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions." *Jones*, 565 U.S. at 427 (Alito, J., concurring in the judgment). The Fourth Amendment cannot prevent private parties from collecting and using data about their customers, but "[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.* at 429-430. If Congress and state legislatures share petitioner's concern about the type and quantity of information collected by cell-service providers and other third parties, those legislators can pass laws to limit the collection, use, or dissemination of that data. Rather than distort or arbitrarily limit Fourth Amendment doctrine, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id.* at 429.

Even absent action by the legislature, the public may persuade third-party providers to alter their conduct to protect privacy interests. Providers' decisions to keep records of tower usage spanning months or years stems not from technological necessity, but from business con-

siderations. Companies thus may yield to customer demands for privacy. See, *e.g.*, EPIC Amicus Br. 31-34 (describing how Apple altered the location data it collected after facing a public backlash to its "surreptitious location tracking"); *Fifth Circuit In re Application*, 724 F.3d at 615 ("[C]ell phone users may reasonably want their location information to remain private, * * * [b]ut 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."). A variety of constraints accordingly may shield certain information conveyed to a third party from further disclosure.

B. The Government Did Not Obtain The Cell-Site Records By Trespassing On A Constitutionally Protected Area

Petitioner alternatively contends (Br. 32) that the government's acquisition of his providers' cell-site records impermissibly intruded on his private papers under "[a] property-based [Fourth Amendment] analysis." That argument is not properly presented here because petitioner did not press it below, the court of appeals did not pass upon it, and petitioner did not raise the claim in his petition for a writ of certiorari. See *Jones*, 565 U.S. at 413. In any event, petitioner's argument that the government's acquisition of historical cell-site records constituted a trespassory search lacks merit.

1. Petitioner's property-based argument falters at the first step because he cannot establish a cognizable property interest in his providers' records of which cell towers they used to connect his calls. Petitioner did not create those records and has no right to control their content. Although petitioner now maintains (Br. 32-35)

that the providers' cell-site records are his own "papers" or "effects," he "stipulate[d] and agree[d]" at trial that they instead were "authentic and accurate business records of [MetroPCS and Sprint]." J.A. 51; see *Christian Legal Soc'y* v. *Martinez*, 561 U.S. 661, 677 (2010) (parties are "bound by the factual stipulations [they] submit[]").

In asserting that he has a property interest in his providers' cell-site records, petitioner again relies on 47 U.S.C. 222, which he maintains prohibits disclosure of cell-site information "without 'express prior authorization of the customer.'" Pet. Br. 11 (citation omitted). As explained, pp. 21-22, *supra*, petitioner misreads the statute: Section 222 permits disclosure of cell-site records in a variety of circumstances without a customer's consent. 47 U.S.C. 222(c)(1) and (d)(1)-(4). The statute accordingly cannot bear the weight petitioner places on it in his novel attempt to establish that he has property rights in his providers' business records. See Pamela Samuelson, *Privacy As Intellectual Property*, 52 Stan. L. Rev. 1125, 1130-1131 (2000) ("Although the law often protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such.") (footnote omitted).

2. Even if Section 222 created certain property rights in cell-site information, petitioner cannot establish that the government's acquisition of the records invades any interest protected by the statute. Section 222 authorizes disclosure of cell-site records without the customer's consent in accordance with the SCA. See 47 U.S.C. 222(c)(1) (permitting disclosure "as required by law"). And cell-service providers expressly reserve

their rights to collect cell-site information and disclose that data in response to court orders. See p. 3 n.1, *supra* (citing privacy policies). The government's acquisition of the providers' business records is therefore consistent with any conceivable property rights petitioner might have in those records.

II. IF THE GOVERNMENT'S ACQUISITION OF CELL-SITE RECORDS WAS A SEARCH OF PETITIONER, IT WAS REASONABLE UNDER THE FOURTH AMENDMENT

Even if petitioner could establish that the government's acquisition of MetroPCS's and Sprint's business records pursuant to an SCA order qualified as a Fourth Amendment search of him, the government's action was constitutionally reasonable.[11] As this Court recently observed, "[t]he Fourth Amendment's proper function is to constrain, not against all intrusions as such, but against intrusions which are not justified in the circumstances, or which are made in an improper manner." *Maryland* v. *King*, 133 S. Ct. 1958, 1969 (2013) (brackets in original; citation omitted). Thus, "[a]s the text of

---

[11] Petitioner suggests (Br. 48) that the Court avoid decision on this issue and instead remand for the court of appeals to consider whether any search of him was reasonable. But the question presented asks whether the Fourth Amendment permits the government to acquire cell-site records without a warrant, Pet. i, and that question cannot be answered without resolving whether any search was constitutionally reasonable. The government raised the reasonableness argument below and in its brief in opposition, see Gov't C.A. Br. 37-40; Br. in Opp. 22-26, and that issue accordingly is properly presented here. See *Granfinanciera, S. A.* v. *Nordberg,* 492 U.S. 33, 38–39 (1989). The Eleventh Circuit has agreed with the government's position that the warrantless acquisition of historical cell-site records is reasonable. See *Davis*, 785 F.3d at 516-518. The Court should resolve that question to provide "clear guidance to law enforcement." *Riley*, 134 S. Ct. at 2491.

the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" *Ibid.* (citation omitted).

Applying that standard here, the Fourth Amendment permits the government's acquisition of cell-site records pursuant to a judicial order authorized by the SCA. That action falls within the well-recognized permissibility of using compulsory process to obtain information. And a traditional balance of interests further demonstrates that the government's conduct was reasonable.

A. Law Enforcement Agents Need Not Obtain A Warrant To Conduct Searches Using Compulsory Process

1. This Court has long recognized that the Fourth Amendment applies to the use of subpoenas and other forms of government action that result in "the orderly taking under compulsion of process." *United States* v. *Morton Salt Co.*, 338 U.S. 632, 652 (1950); see, *e.g.*, *United States* v. *Dionisio*, 410 U.S. 1, 11-12 (1973) (grand jury subpoena); *McPhaul* v. *United States*, 364 U.S. 372, 382-383 (1960) (legislative subpoena); *Oklahoma Press Publ'g Co.* v. *Walling*, 327 U.S. 186, 208-209 (1946) (*Oklahoma Press*) (administrative subpoena). In applying the Fourth Amendment reasonableness standard in this context, the Court has concluded that subpoenas for records do not require a warrant based on probable cause, even when challenged by the party to whom the records belong. See *Miller*, 425 U.S. at 446; see also *Oklahoma Press*, 327 U.S. at 208-209. Instead, the Fourth Amendment permits the government to acquire documents by subpoena so long as "the investigation is authorized by Congress, is for a purpose Congress can order, * * * the documents sought are rele-

vant to the inquiry," and the "specification of the documents to be produced [is] adequate, but not excessive, for the purposes of the relevant inquiry." *Oklahoma Press*, 327 U.S. at 209; see *Donovan* v. *Lone Steer, Inc.*, 464 U.S. 408, 415 (1984) ("[T]he Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.") (citation omitted).

The Court has identified several reasons why the Fourth Amendment does not require a warrant for the government to obtain evidence using compulsory process. That conduct represents a lesser degree of intrusion than the kinds of searches that typically require a warrant because the subpoena recipient rather than the government finds and produces the record. See *Donovan*, 464 U.S. at 414 (observing that governmental action in "mak[ing] nonconsensual entries into areas not open to the public" is "quite different from * * * governmental action" in seeking the production of records); see also *Dionisio*, 410 U.S. at 10. In addition, the subpoena recipient has an "opportunity to present objections" before producing the records, which further minimizes the intrusion. *Oklahoma Press*, 327 U.S. at 195; see *Donovan*, 464 U.S. at 416; see also *City of Los Angeles* v. *Patel*, 135 S. Ct. 2443, 2453-2454 (2015) (explaining the benefits of pre-compliance review).

On the other side of the balance, the Court has recognized that the government has a significant interest in acquiring records through compulsory process at the early stage of an investigation, before probable cause exists to support issuance of a warrant. See *Oklahoma Press*, 327 U.S. at 213 (observing that a warrant requirement in this context "would stop much if not all of

investigation in the public interest at the threshold of inquiry," rendering it "substantially impossible" to "effective[ly] discharge * * * the duties of investigation"). The government's ability to investigate and prosecute crime would be severely hindered if it were "required to justify the issuance of a * * * subpoena by presenting evidence sufficient to establish probable cause" when "the very purpose of requesting the information is to ascertain whether probable cause exists." *United States* v. *R. Enterprises, Inc.*, 498 U.S. 292, 297 (1991). This Court has accordingly recognized that the use of a subpoena to obtain a third party's records pertaining to an individual is "a proper and long-standing law enforcement technique" that "does not violate the Fourth Amendment rights of [the individual] under investigation." *Miller*, 425 U.S. at 444.

2. The government's acquisition of cell-site records pursuant to a court order authorized by the SCA falls within the authority this Court has recognized for "subpoena[s] or order[s] authorized by law and safeguarded by judicial sanction." *Oklahoma Press*, 327 U.S. at 208. Section 2703(d) orders share the same features as other forms of compulsory process that have prompted the Court to find Fourth Amendment requirements satisfied without a warrant: the recipient, not the government, locates and produces the records; the recipient may challenge the order in court before complying, see 18 U.S.C. 2703(d); and the government often relies on Section 2703(d) orders at the preliminary stage of an investigation before it has developed probable cause.

Indeed, the SCA provides substantially greater privacy protections than an ordinary subpoena. See *Davis*, 785 F.3d at 505-506 (describing SCA privacy-protection provisions). In particular, Section 2703(d) "raises the

bar" as compared to other forms of compulsory process by requiring the government to establish "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*, 785 F.3d at 505-506. The SCA provides further protection by requiring court approval, which ensures that a neutral judicial officer agrees that the request is appropriate in scope and justification. Because "[t]he SCA goes above and beyond the constitutional requirements regarding compulsory subpoena process," *id.* at 506, the government's acquisition of business records pursuant to a valid Section 2703(d) order does not violate the Fourth Amendment.

3. Petitioner contends (Br. 51-53) that the Fourth Amendment permits the warrantless acquisition of a third party's records pursuant to subpoena only when an individual to whom the records pertain holds no "reasonable expectation of privacy" in the records. This Court's cases do not support petitioner's proposed limitation, and acceptance of his argument would impose serious burdens on investigations.

Petitioner identifies no case in which this Court has held that certain classes of business records are exempt from the subpoena standard because they contain sensitive information about the business's customers.[12]

---

[12] Although petitioner acknowledges (Br. 52) that the Court has permitted the government to subpoena third parties for records pertaining to their customers, he contends that the customers had no legitimate privacy expectation. But that is because the Court applied the third-party doctrine, which equally establishes here that petitioner has no Fourth Amendment privacy expectation is his cell-service providers' records. See pp. 15-41, *supra*.

The subpoena standard itself may impose more stringent requirements depending on the nature of the requested documents. See *Oklahoma Press*, 327 U.S. at 209 ("[R]elevancy and adequacy or excess in the breadth of the subpoena are matters variable in relation to the nature, purposes and scope of the inquiry."). For example, "[s]pecial problems of privacy * * * might be presented by subpoena of a personal diary," which would necessitate a careful review to ensure the subpoena is "narrowly drawn and seek[s] only documents of unquestionable relevance." *Fisher* v. *United States*, 425 U.S. 391, 401 n.7 (1976); see *United States* v. *Bennett*, 409 F.2d 888, 897 (2d Cir. 1969) (Friendly, J.) (distinguishing between a personal diary that may contain large quantities of irrelevant information and a diary "whose cover page bore the title 'Robberies I Have Performed'"), cited by *Fisher*, 425 U.S. at 401 n.7. But courts have rejected petitioner's contention that a warrant is required to subpoena sensitive records held by third parties, instead holding that the subpoena standard's reasonableness requirement sufficiently safeguards any privacy expectations that exist. See, *e.g.*, *United States* v. *Zadeh*, 820 F.3d 746, 758 (5th Cir. 2016) (upholding subpoena for a physician's medical records that "implicat[ed] privacy interests of patients," but "narrowly confining the scope of production to the ongoing government investigation and placing all produced medical records under seal"); *In re Subpoena Duces Tecum*, 228 F.3d 341, 349 (4th Cir. 2000) (rejecting challenge to subpoena for medical records, but observing that "[t]he value of constraining governmental power, which [the physician] has urged through his misplaced probable cause argument, is nevertheless recognized in the judicial supervision of subpoenas").

Petitioner suggests (Br. 52) that Section 2703(d) orders are unreasonable because the government need not provide notice to the individual to whom the records pertain. As a general matter, this Court has rejected the argument that the Fourth Amendment requires "notice of subpoenas issued to third parties * * * to allow a target to prevent an unconstitutional search or seizure." *SEC*, 467 U.S. at 743. Even if a target has a limited expectation of privacy in records held by a third party, courts can accommodate that interest when assessing the justification and scope of a request for information, as Section 2703(d) requires. Judicial authorization in advance of the intrusion provides appropriate protection when notice to the target would frustrate the investigative purpose. See, *e.g.*, *Dalia* v. *United States*, 441 U.S. 238, 247-248 (1979). And altering the Fourth Amendment standard to require a warrant would not address petitioner's notice concern. The warrant would be served on the provider, not the target, and in any event, notice of a warrant is neither an inflexible Fourth Amendment requirement, see *Katz*, 389 U.S. at 355 n.16, nor a basis for a pre-enforcement challenge, see *United States* v. *Grubbs*, 547 U.S. 90, 98-99 (2006).

Petitioner's proposed revision of the constitutional standard for subpoenas would impede longstanding investigative practices. This Court has recognized that the government's use of compulsory process is "necessary to the administration of justice." *Dionisio*, 410 U.S. at 10 (citation omitted). Petitioner himself shrinks from the extreme implications of his argument, suggesting (Br. 53 n.40) that "the Court need not address whether different rules are appropriate for subpoenas issued by a grand jury." But the Court has held that administrative subpoenas are analogous to their grand-

jury counterparts, *Morton Salt*, 338 U.S. at 642-643, and has applied the same constitutional standard to all forms of compulsory process, *Dionisio*, 410 U.S. at 10-11. The reasonableness standard that applies to subpoenas demonstrates that the government did not violate the Fourth Amendment in obtaining business records pursuant to a valid order under Section 2703(d).

B. A Traditional Balancing Of Interests Further Supports The Constitutionality Of A Section 2703(d) Order

Traditional standards of Fourth Amendment reasonableness independently confirm that a Section 2703(d) court order is a reasonable mechanism for obtaining historical cell-site records. In deciding whether a warrantless search is permissible, this Court "balance[s] the privacy-related and law enforcement-related concerns to determine if the intrusion was reasonable." *King*, 133 S. Ct. at 1970 (citation omitted). Congress struck a constitutionally permissible balance in enacting the SCA.

1. As discussed above, under traditional Fourth Amendment standards, petitioner had no legitimate expectation of privacy in the third-party business records at issue here. But even if this Court were to depart from that settled framework, petitioner could at most assert only a diminished expectation of privacy in those records. Cf. Pet. Br. 38 (treating disclosure of information to a third party as "one factor" that affects privacy expectations). Petitioner did not create the records, he does not possess them, and he has no control over their contents.

To the extent the providers' collection of information about petitioner's proximity to their cell towers infringed his privacy expectations, that conduct occurred

without governmental involvement. And the government's subsequent acquisition of the providers' records in accordance with Section 2703(d) constituted an "orderly taking under compulsion of process." *Morton Salt*, 338 U.S. at 652. The statutory protections in the SCA further minimized any privacy invasion by prohibiting "[a]ny willful disclosure" of cell-site information not "made in the proper performance of" governmental functions. 18 U.S.C. 2707(g); see *King*, 133 S. Ct. at 1980 (noting that "a statutory or regulatory duty to avoid unwarranted disclosures generally allays . . . privacy concerns") (citation and internal quotation marks omitted). The use of a Section 2703(d) order to obtain cell-service providers' business records thus involves a "minimal intrusion[]" and "diminished expectations of privacy"—both of which "may render a warrantless search or seizure reasonable." *King*, 133 S. Ct. at 1969 (citation omitted).

2. On the other side of the reasonableness balance, the government has a compelling interest in obtaining cell-site records using a Section 2703(d) court order, rather than a warrant, because, like other investigative techniques that involve seeking information about a crime from third parties, this evidence is "particularly valuable during the early stages of an investigation, when the police [may] lack probable cause and are confronted with multiple suspects." *Davis*, 785 F.3d at 518. "[Section] 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." *Ibid.*

Examples illustrate the important role cell-site information plays in helping law enforcement agents develop leads and solve crimes. In one case, the FBI determined that someone was using a home computer to distribute and download child pornography, but each of the four adults who regularly used that computer denied responsibility for the crime. See *United States* v. *Reynolds*, 626 Fed. Appx. 610, 612 (6th Cir. 2015), petition for cert. pending, No. 16-8574 (filed Dec. 10, 2015). The FBI obtained cell-site records that revealed that three of the four adults used cell towers that were "geographically inconsistent" with their being near the computer at times when child pornography was downloaded, while the fourth adult "used cell towers that were consistent with his being at the residence during the download periods." *Ibid.* The records accordingly helped the government eliminate three suspects and identify the perpetrator.

In another example, cell-site records helped investigators identify the person who shot into the home of a federal judge. "The police had no eyewitnesses and a very large pool of suspects, including many litigants and defendants who had appeared before the judge," but with the aid of court-issued orders for cell-site information pertaining to some "possible suspects," the police acquired "a general idea of the location of the phones," which "allowed agents to exclude certain innocent people and pursue leads that eventually led to the arrest of the alleged shooter." *Geolocation Technology and Privacy: Hearing Before the H. Comm. on Oversight and Government Reform*, 114th Cong., 2d Sess. 4-5 (2016) (statement of Richard Downing, Acting DAAG, Computer Crime and Intellectual Property Section, U.S. Department of Justice).

States and the federal government unquestionably have an "interest in apprehending violators," *United States* v. *Knights*, 534 U.S. 112, 121 (2001), and in doing so as quickly as possible. See *United States* v. *Salerno*, 481 U.S. 739, 750-751 (1987). Bringing the guilty to justice vindicates the law, protects the public, and provides closure to victims. These benefits lie at the very heart of the government's responsibility to maintain order and shield its citizens from harm—and they support the reasonableness of the SCA orders at issue here.

3. That conclusion gains additional force from the legislative judgment embodied by the SCA. This Court has "be[en] reluctant to decide that a search * * * authorized by Congress was unreasonable," *United States* v. *Di Re*, 332 U.S. 581, 585 (1948), particularly when "nothing in the Court's prior cases indicat[es] that under the Fourth Amendment a warrant is required," *United States* v. *Watson*, 423 U.S. 411, 416-417 (1976). In enacting the SCA, Congress specifically considered Fourth Amendment principles and this Court's precedents. See H.R. Rep. No. 647, 99th Cong., 2d Sess. 72 (1986) (1986 House Report) (observing that "records maintained by third parties" generally "have no special privacy or confidentiality protection"). Congress selected the Section 2703(d) standard after determining that "an intermediate standard" that is "higher than a subpoena, but not a probable cause warrant" would "guard against 'fishing expeditions' by law enforcement" while ensuring access to cell-service providers' records pertaining to their customers in appropriate circumstances. H.R. Rep. No. 827, 103d Cong., 2d Sess. Pt. 1, at 31 (1994). The SCA thus "represents a judgment by Congress that it is not unreasonable under the Fourth Amendment" for the government to obtain cell-

site records in accordance with the statutory procedures Congress enacted—a consideration entitled to significant weight. *Watson*, 423 U.S. at 415; see *Jones*, 565 U.S. at 429-430 (Alito, J., concurring in the judgment).

Petitioner contends (Br. 50) that Congress may not have "anticipate[d] the contemporary ubiquity of cell phones" when it chose the Section 2703(d) standard. But Congress designed the statute to respond to "dramatic changes in new computer and telecommunications technologies," which it recognized included cell phones. S. Rep. No. 541, 99th Cong., 2d Sess. 1-2 (1986) (Senate Report); see 1986 House Report 18. Congress understood that cell-phone technology works by "send[ing] signals over the air on a radio frequency to a cell site." 1986 House Report 20; Senate Report 9. And Congress specifically applied the Section 2703(d) standard to all non-content records cell-service providers might keep pertaining to their customers, concluding that the standard "represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." Senate Report 5.

Congress has had numerous opportunities to reconsider the balance it struck in Section 2703(d)—including as applied specifically to cell-site information.[13] In 2000, for example, Congress considered—but ultimately did not enact—a bill that would have amended Section 2703

---

[13] Congress did alter the Section 2703(d) standard in 1994 to make it harder for the government to obtain non-content records by requiring the government to offer "specific and articulable facts" and seek only records that may be "material" to an ongoing investigation. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, Tit. II, § 207(a), 108 Stat. 4292.

to require a showing of probable cause for "mobile electronic information generated by and disclosing the current physical location of a subscriber's equipment." Digital Privacy Act of 2000, H.R. 4987, 106th Cong., 2d Sess. § 6, at 4 (2000). And earlier this year, the House referred a bill to committee that would allow the government to obtain cell-site records using search warrants but not Section 2703(d) orders. See Geolocation Privacy and Surveillance Act, H.R. 1062, 115th Cong., 1st Sess. §§ 2, 5 (2017). Congress considered similar proposals in prior iterations of that bill. See, *e.g.*, Geolocational Privacy and Surveillance Act, S. 237, 114th Cong., 1st Sess. §§ 2, 5 (2015); Geolocational Privacy and Surveillance Act, H.R. 1312, 113th Cong., 1st Sess. §§ 2, 5 (2013). Congress's continued attention to the appropriate balance between privacy interests and the needs of law enforcement in the face of rapidly evolving technology reinforces the reasonableness of the Section 2703(d) standard.

III. PETITIONER CORRECTLY CONCEDES THAT THE GOVERNMENT DOES NOT VIOLATE THE FOURTH AMENDMENT BY ACQUIRING SHORTER-TERM CELL-SITE RECORDS

For the reasons set forth above, the court of appeals correctly held that the government's warrantless acquisition of all the cell-site records pertaining to petitioner's phone complied with the Fourth Amendment.[14] But if the Court were to conclude that requests for long-

[14] If the Court disagrees and concludes that the government violated petitioner's Fourth Amendment rights it should remand to allow the court of appeals to consider the government's arguments that the good-faith exception to the exclusionary rule applies and that any error in admitting the cell-site data was harmless. See Gov't C.A. Br. 40-47.

term cell-site data require a warrant, it should confirm that the Section 2703(d) order directed at Sprint—which sought seven days of records and resulted in the production of two days of data—was constitutional.

Petitioner acknowledges that "there is some period of time for which the government may obtain a person's historical [cell-site information] free from Fourth Amendment scrutiny, because the duration is too brief to implicate the person's reasonable privacy interest." Br. 30 (brackets, citation, and internal quotation marks omitted). That concession follows from petitioner's recognition (Br. 30-31) that investigators using traditional surveillance techniques frequently obtain information about an individual's location and movements during discrete time periods. "[R]elatively short-term monitoring of a person's movements" therefore "accords with expectations of privacy that our society has recognized as reasonable." *Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment).

Applying that analysis, agents did not need a warrant to request seven days of cell-site information from Sprint. Law enforcement agents regularly surveil suspects for a week or more. See, *e.g.*, *Young* v. *Owens*, 577 Fed. Appx. 410, 412 (6th Cir. 2014) ("[s]everal weeks of surveillance" of a store); *United States* v. *Gaskins*, 690 F.3d 569, 574, 577 (D.C. Cir. 2012) ("weeks of surveillance" of "numerous locations * * * using stationary vans, moving cars, and a mounted pole camera"); *United States* v. *Johnson*, 480 Fed. Appx. 835, 837 (6th Cir. 2012) (suspect's residence was under visual surveillance "for five to six weeks and he was seen there on a daily basis"); *United States* v. *Gramlich*, 551 F.2d 1359, 1360-1361 & n.7, 1362 (5th Cir.) ("continual surveillance of [defendant's] activities" for "over three weeks"), cert.

denied, 434 U.S. 866 (1977); *Shades Ridge Holding Co.* v. *Commissioner of Internal Revenue*, 23 T.C.M. (CCH) 1665 (1964) ("close surveillance of [suspect] and of his activities" that "often was continuous, all day, for 6 days a week" over several months).

Using traditional techniques, officers can acquire extensive information about an individual's movements. In one case, for example, officers conducted "more than one week of detailed surveillance" and determined that the suspect's movements "followed a set pattern" that included his departure from his home in a particular make of car; his arrival at a nearby building where "he would place window tinting film on his car windows"; his entrance on "Interstate 64 westbound toward Mechanicsville"; his exit from the interstate, where he affixed "a new license plate"; his return on the same interstate; his "driv[ing] back and forth on Route 360, stopping in parking lots adjacent to two different banks but never exiting his car"; and then finally his returning home. *United States* v. *Caraballo*, 384 Fed. Appx. 285, 287-288, 290 (4th Cir. 2010) (per curiam). The seven days of cell-site information from Sprint here—which contained far less precise location information—surely threatened no greater intrusion on petitioner's asserted privacy interests (and probably far less) than what officers could have obtained "using previously available techniques." *Jones*, 565 U.S. at 431 (Alito, J., concurring in the judgment). In no circumstance, therefore, did the Section 2703(d) order directed at Sprint violate the Fourth Amendment.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General
KENNETH A. BLANCO
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
ELIZABETH B. PRELOGAR
Assistant to the Solicitor General
JENNY C. ELLICKSON
Attorney

SEPTEMBER 2017

APPENDIX A

1. U.S. Const. Amend. IV provides:

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.

2. 18 U.S.C. 2703 provides:

Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a sub-

scriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional

90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

3. 47 U.S.C. 222 provides:

Privacy of customer information

(a) In general

Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.

(b) Confidentiality of carrier information

A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) Confidentiality of customer proprietary network information

(1) Privacy requirements for telecommunications carriers

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

(2) Disclosure on request by customers

A telecommunications carrier shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) Aggregate customer information

A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on

reasonable and nondiscriminatory terms and conditions upon reasonable request therefor.

(d) Exceptions

Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services;

(3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title)—

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) Subscriber list information

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) Authority to use location information

For purposes of subsection (c)(1) of this section, without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d) of this title) or the user of an IP-enabled voice service (as such term is defined in section 615b of this title), other than in accordance with subsection (d)(4) of this section; or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) Subscriber listed and unlisted information for emergency services

Notwithstanding subsections (b), (c), and (d) of this section, a telecommunications carrier that provides telephone exchange service or a provider of IP-enabled voice service (as such term is defined in section 615b of this title) shall provide information described in subsection (i)(3)(A)[1] of this section (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

(h) Definitions

As used in this section:

(1) Customer proprietary network information

The term "customer proprietary network information" means—

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecom-

---

[1] So in original. Probably should be subsection "(h)(3)(A)".

munications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and

(B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.

(2) Aggregate information

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) Subscriber list information

The term "subscriber list information" means any information—

(A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) Public safety answering point

The term "public safety answering point" means a facility that has been designated to receive emer-

gency calls and route them to emergency service personnel.

(5) Emergency services

The term "emergency services" means 9-1-1 emergency services and emergency notification services.

(6) Emergency notification services

The term "emergency notification services" means services that notify the public of an emergency.

(7) Emergency support services

The term "emergency support services" means information or data base management services used in support of emergency services.

APPENDIX B

The illustrative map in Figure 2 at p. 26, *supra*, is intended to show the approximate density and variety of establishments in the area where cell-site records placed petitioner's phone around the time of a robbery of a Radio Shack at 13330 E. Jefferson Ave., Detroit, Michigan, 48215, on December 13, 2010. See Pet. App. 80a-82a, 86a; see also J.A. 57-60 (testimony explaining the creation of the map appearing in Government Exhibit 57, reproduced at Pet. App. 86a). The illustrative map was created using Google Maps' My Maps tool. See https://www.google.com/maps/about/mymaps/. It reflects Google's map, satellite, and directory information as of September 25, 2017.

The illustration covers the region between two cell towers that petitioner's phone connected to the morning of the robbery, based on the cell tower and sector locations from the government's trial exhibit reproduced at Pet. App. 86a; see also p. 25, *supra* (reproducing a portion of that exhibit). The locations of the cell towers and the lines depicting the cell sectors in the illustrative map are based on their locations on the exhibit at Pet. App. 86a. The cell towers' coverage area shown on the illustrative map is approximate.

The icons on the map represent establishments in that area, based on Google Maps' satellite imagery and directory labels. Buildings not labeled by Google were identified from Google's satellite and street imagery; most were single-family homes or apartment buildings. Buildings or structures that appeared to be empty or abandoned were not counted, such that the illustrative map errs on the side of under-inclusion.