No. 16-6761

IN THE SUPREME COURT OF THE UNITED STATES

FRANK CAIRA, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

NOEL J. FRANCISCO
Acting Solicitor General
Counsel of Record

KENNETH A. BLANCO
Acting Assistant Attorney 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 subpoena issued in accordance with 18 U.S.C. 2703(c)(2), of internet-protocol-address records created and maintained by an email-service provider violates the Fourth Amendment rights of the individual email user to whom the records pertain.

IN THE SUPREME COURT OF THE UNITED STATES

No. 16-6761

FRANK CAIRA, PETITIONER

v.

UNITED STATES OF AMERICA

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT

BRIEF FOR THE UNITED STATES IN OPPOSITION

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. A1-A4) is reported at 833 F.3d 803. The order of the district court denying petitioner's motion to suppress (Pet. App. B1-B6) is unreported.

JURISDICTION

The judgment of the court of appeals was entered on August 17, 2016. The petition for a writ of certiorari was filed on September 11, 2016. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a guilty plea in the United States District Court for the Northern District of Illinois, petitioner was convicted of conspiracy to manufacture, distribute, and possess with intent to distribute ecstasy, in violation of 21 U.S.C. 846 and 841(b)(1)(C), and conspiracy to manufacture, distribute, and possess with intent to distribute 100 or more marijuana plants, in violation of 21 U.S.C. 846 and 841(b)(1)(B). Judgment 1. The district court sentenced petitioner to 300 months of imprisonment, to be followed by five years of supervised release. Id. at 2-3. The court of appeals affirmed. Pet. App. A1-A4.

1. a. In 2005, petitioner and co-conspirator Jonathan Stoffels agreed to manufacture ecstasy for distribution. D. Ct. Doc. 242, at 3 (Mar. 8, 2013) (Plea Agreement). Petitioner found the recipe for ecstasy on the Internet and procured the necessary ingredients and supplies, including sassafras oil, which is a List 1 controlled substance. Ibid. From 2005 to 2008, petitioner and Stoffels purchased sassafras oil from several online vendors and manufactured ecstasy in various locations in the Chicago area. Id. at 3-4. During the same period, Stoffels sold the ecstasy to customers and split the proceeds with petitioner. Id. at 4.

In 2008, petitioner, Stoffels, and other co-conspirators agreed to grow marijuana plants for distribution. Plea Agreement 4. Petitioner purchased marijuana seeds from an online vendor and

rented a house for the purpose of growing marijuana plants in the basement. Id. at 4-5. Petitioner and his co-conspirators purchased the equipment necessary to grow marijuana indoors and ultimately grew and maintained marijuana plants in two different locations. Id. at 5.

b. In 2008, petitioner used the email address gslabs@hotmail.com to contact a Vietnamese website in an attempt to purchase sassafras oil. Pet. App. A1. The Drug Enforcement Administration (DEA) had been monitoring that website. Ibid. In accordance with the Stored Communications Act (SCA), 18 U.S.C. 2701 et seq., the DEA issued an administrative subpoena to Microsoft Corporation (Microsoft), which owns the web-based Hotmail email service. Pet. App. A1; see 18 U.S.C. 2703(c)(2). The subpoena directed Microsoft to produce specified records for the gslabs@hotmail.com address, including account login histories containing the internet-protocol (IP) addresses associated with the computers that were used to access the account. Pet. App. A1-A2.

The SCA generally prohibits communications providers from disclosing certain records pertaining to their subscribers, but permits the government to acquire such records in certain circumstances. 18 U.S.C. 2510(1), 2702, 2703, 2711(1). As relevant here, the government may "use[] an administrative subpoena" to obtain the name, address, "telephone or instrument

number or other subscriber number or identity, including any temporarily assigned network address," and "records of session times and durations" pertaining to a subscriber. 18 U.S.C. 2703(c)(2).

In response to the administrative subpoena, "Microsoft gave the DEA information about instances in which the gslabs@hotmail.com account was accessed between July 5 and September 15, 2008." Pet. App. A2. For each account login, Microsoft provided the date, time, and IP address associated with the computer that was used to access the account. Ibid.

The DEA reviewed those records and noticed that a computer using the IP address 24.15.180.222 had frequently accessed the gslabs@hotmail.com account. Pet. App. 2a. After determining that Comcast Corporation (Comcast), an internet service provider, owned that IP address, the DEA sent Comcast an administrative subpoena requesting information associated with the IP address, including the subscriber's name and address. Ibid. In response, Comcast gave the DEA the name and address of petitioner's wife, who had been assigned that IP address. Ibid. After further investigation, petitioner was charged with various drug offenses. Ibid.; see id. at B1.

2. a. "[I]n an attempt to avoid conviction" on the drug charges in this case, petitioner "tried to have the prosecutor and DEA agent murdered." Pet. App. A4; see United States v. Caira,

737 F.3d 455, 458-461 (7th Cir. 2013) (describing the murder scheme in detail), cert. denied, 135 S. Ct. 151 (2015). Based on that conduct, a jury convicted petitioner on two counts each of conspiracy to commit murder of a United States official, in violation of 18 U.S.C. 1117, and solicitation of a violent felony, in violation of 18 U.S.C. 373. Caira, 737 F.3d at 458. Petitioner was sentenced to a term of life in prison plus 20 years for those offenses. Id. at 460.

b. After petitioner was convicted on the charges arising from the murder plot, he moved in this case to suppress evidence obtained through the administrative subpoenas. Pet. App. A2. Petitioner argued that the Fourth Amendment required the government to use a warrant to obtain that information. Ibid.

The district court denied the suppression motion. Pet. App. B1-B6. The court observed that "federal courts that have addressed the issue have routinely held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation.'" Id. at B5 (quoting United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008)). The court cited cases holding that "[s]uch information * * * is voluntarily provided to third parties and [is] therefore exempt from Fourth Amendment analysis." Id. at B3. The court accordingly concluded that suppression was not warranted. Id. at B5-B6.

c. Petitioner then pleaded guilty to one count of conspiracy to manufacture, distribute, and possess with intent to distribute ecstasy, in violation of 21 U.S.C. 846 and 841(b)(1)(C), and one count of conspiracy to manufacture, distribute, and possess with intent to distribute 100 or more marijuana plants, in violation of 21 U.S.C. 846 and 841(b)(1)(B). Judgment 1. Petitioner reserved the right to appeal the denial of his motion to suppress. Pet. App. A2. The district court sentenced petitioner to 300 months of imprisonment, to be followed by five years of supervised release. Judgment 2-3.

d. The court of appeals affirmed. Pet. App. A1-A4. As relevant here, the court held that the government's acquisition of Microsoft's IP-address records did not violate petitioner's Fourth Amendment rights. Id. at A1. The court concluded that petitioner "did not have a reasonable expectation of privacy" in the IP addresses he used to log in to the gslabs@hotmail.com account because he "voluntarily shared the relevant information with" Microsoft, which created and maintained records of the transactions. Ibid.

Relying on this Court's decisions in Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976), the court of appeals explained that "[i]n what has come to be known as the 'third-party doctrine,' th[is] Court held that 'a person has no legitimate expectation of privacy in information he

voluntarily turns over to third parties . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." Pet. App. A2 (quoting Smith, 442 U.S. at 743-744). In Smith, the court of appeals observed, this Court rejected a defendant's challenge to the government's use of a pen register to record the phone numbers dialed from his home telephone because "as a necessary step in placing phone calls, he shared that information with the phone company." Ibid. Miller, the court of appeals explained, likewise held that a bank customer had no Fourth Amendment privacy interest in bank records reflecting his financial transactions, "even though they contained sensitive financial information, because [the customer] had voluntarily shared that information with a third party -- the bank." Ibid.

The court of appeals concluded that petitioner similarly lacked a reasonable expectation of privacy in Microsoft's IP-address records because he "voluntarily shared" his IP address with Microsoft each time he used a computer to log in to his Hotmail email account. Pet. App. A4; see id. at A3. The court rejected petitioner's reliance on United States v. Jones, 565 U.S. 400 (2012), which held that the government's installation of a Global-Positioning-System (GPS) tracking device on a vehicle constituted a search under the Fourth Amendment, id. at 405. Pet. App. A3-A4. The court observed that "Jones did not do away with

the third-party doctrine" and "had no occasion to" do so because the government there had not obtained information voluntarily conveyed to a third party but instead "used its own GPS device to track Jones's location." Id. at A4. The court also explained that the IP-address information obtained in this case is not similar to the GPS tracking data at issue in Jones because IP-address records do not reveal or "monitor 'every single movement'" an individual makes. Ibid. (quoting Jones, 565 U.S. at 430 (Alito, J., concurring in the judgment)). Because petitioner lacked a reasonable expectation of privacy in Microsoft's IP-address records, the court concluded that "the DEA committed no Fourth Amendment 'search' when it subpoenaed that information." Ibid.

ARGUMENT

Petitioner renews his claim (Pet. 9-23) that the government violated the Fourth Amendment when it acquired Microsoft's IP-address records pursuant to an administrative subpoena obtained in accordance with the SCA.[1] Petitioner further asserts (Pet. 9) that this case implicates a "circuit split * * * on whether the third-party doctrine is still applicable today." Those claims lack merit. The court of appeals correctly concluded that the Fourth Amendment permits the government to obtain IP-address records from

[1] Petitioner does not independently challenge the Comcast subpoena, which required Comcast to disclose the name and home address of the customer who was assigned the IP address that most frequently was used to log in to petitioner's email account. See Pet. 13-22.

a third party pursuant to an administrative subpoena, and no conflict exists on that question or on any broader question about the continuing validity of this Court's third-party precedents. In any event, this case would be an unsuitable vehicle to address the Fourth Amendment question because the relevant evidence is admissible under the good-faith exception to the exclusionary rule. Further review is not warranted.

1. The court of appeals correctly held that the government's acquisition of Microsoft's IP-address records did not violate petitioner's Fourth Amendment rights. Petitioner has no interest protected by the Fourth Amendment in those business records. And even if he did have such an interest, the SCA procedure, which contemplates that IP-address information may be obtained pursuant to an administrative subpoena, is constitutionally reasonable.

a. A person has no Fourth Amendment interest in records created by a communications-service provider in the ordinary course of business that pertain to the individual's transactions with the service provider.

i. The Fourth Amendment's prohibition on unreasonable searches was originally understood to be "tied to common-law trespass." United States v. Jones, 565 U.S. 400, 405 (2012). Since this Court's decision in Katz v. United States, 389 U.S. 347 (1967), however, the Court has held that a Fourth Amendment search

may also "occur[] when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001).

The Fourth Amendment permits the government to obtain business records through a subpoena, without either a warrant or a showing of probable cause. See Oklahoma Press Publ'g Co. v. Walling, 327 U.S. 186, 194-195 (1946); see also United States v. Miller, 425 U.S. 435, 445-446 (1976). In its decisions in Miller and Smith v. Maryland, 442 U.S. 735 (1979), this Court further concluded that the acquisition of a business's records does not constitute a Fourth Amendment "search" of an individual customer even when the records reflect information pertaining to that customer.

In Miller, the government had obtained by subpoena records of the defendant's accounts from his banks, including copies of his checks, deposit slips, financial statements, and other business records. 425 U.S. at 436-438. The banks were required to keep those records under the Bank Secrecy Act, 12 U.S.C. 1829b(d). 425 U.S. at 436, 440-441. The Court held that the government's acquisition of those records was not an "intrusion into any area in which [the defendant] had a protected Fourth Amendment interest." Id. at 440. The Court explained that the defendant could "assert neither ownership nor possession" of the records; rather, they were "business records of the banks." Ibid. The

Court further rejected the defendant's argument that he had "a reasonable expectation of privacy" in the records because "they [were] merely copies of personal records that were made available to the banks for a limited purpose." Id. at 442. As the Court explained, 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. Because the records obtained from the banks "contained 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 records created by 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 defendant argued that the government's acquisition of the records of his dialed numbers violated his reasonable expectation of privacy and therefore qualified as a Fourth Amendment search. Id. at 741-742. The Court rejected that contention, concluding both that the defendant

lacked a subjective expectation of privacy and that any such expectation was not objectively reasonable. Id. at 742-746.

The Smith Court 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 further emphasized that "the phone company has facilities for recording this information" and "does in fact record this information for a variety of legitimate business purposes." Id. at 743.

The Smith Court 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). That was because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Id. at 743-744 (citing, inter alia, Miller, 425 U.S. at 442-444). "When [the defendant] used his phone," the Court continued, 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). The Court found no more persuasive the defendant's

argument that he reasonably expected the local numbers he dialed to remain private because "telephone companies, in view of their present billing practices, usually do not record local calls" or include those numbers on their customers' monthly bills. Id. at 745. Because the defendant "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record," the Court concluded that he had "assumed the risk that the information would be divulged to police." Ibid.

ii. The court of appeals correctly held that the principles set forth in Miller and Smith resolve this case. See Pet. App. A2-A4.

Petitioner lacks any subjective expectation of privacy in the IP-address records at issue here because they are business records that Microsoft creates for its own purposes. See Pet. App. A2-A3. As with the bank records in Miller, petitioner "can assert neither ownership nor possession" of the IP-address records. 425 U.S. at 440. Rather, Microsoft created and maintained the records as part of the process of providing customers with access to web-based Hotmail email accounts. See Pet. App. A2-A3.

As in Smith, moreover, email users presumably understand that they must send information about the location of the computers they are using to their email providers for the purpose of accessing their email accounts. See Pet. App. A3. As the court of appeals observed, "every time [petitioner] logged in, he sent

Microsoft his I.P. address[] specifically so that Microsoft could send back information to be displayed where [petitioner] was physically present." Ibid. "When [petitioner] used his home computer" to access his Hotmail account, "he expected to see his Hotmail inbox displayed on his home computer screen" -- and "[i]t would have done him no good if his inbox was instead displayed on the screen attached to his computer at work, or a computer at the public library, or the computer he used years earlier when first signing up for a Hotmail account." Ibid. "Although subjective expectations cannot be scientifically gauged," email users do not have a "general expectation" that the IP address they transmit to their email providers to access their accounts "will remain secret." Smith, 442 U.S. at 743.

Additionally, any subjective expectation of privacy in IP-address information conveyed to an email provider 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 number into a phone "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), an email user must reveal the IP address associated with his computer to his email provider in order for the provider to display his inbox on the

screen where he is located. And an email user thus "takes the risk, in revealing his affairs to [the email provider], that the" IP address information he transmits to access his email account "will be conveyed by [the email provider] to the Government." Miller, 425 U.S. at 443. Because petitioner "voluntarily conveyed to [his email provider] information that it had facilities for recording and that it was free to record," he "assumed the risk that the information would be divulged to police." Smith, 442 U.S. at 745. The court of appeals therefore correctly concluded that the government's acquisition of Microsoft's IP-address records did not constitute a Fourth Amendment search.

iii. Petitioner's arguments (Pet. 9-22) to the contrary lack merit.

Petitioner seeks (Pet. 13, 18-22) to avoid the principles set forth in Miller and Smith by contending that email users do not voluntarily convey their IP addresses to their service providers. But "IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." United States v. Forrester, 512 F.3d 500, 510 (9th Cir.), cert. denied, 555 U.S. 908 (2008); see, e.g., United States v. Christie, 624 F.3d 558, 573-574 (3d Cir. 2010), cert. denied, 562 U.S. 1236 (2011); Pet. App. A3. Indeed, petitioner provided his IP address to Microsoft "specifically so that [it] could send back information to be

displayed where [petitioner] was physically present." Pet. App. A3. The court of appeals thus correctly concluded that petitioner "voluntarily shared his I.P. addresses with Microsoft." Id. at A4.

Petitioner also errs in suggesting (Pet. 20) that Smith and Miller are inapplicable because "[t]he nature of information conveyed from IP addresses is much more extensive than the addresses on an envelope, bank deposit records, or call logs from an analog phone." Petitioner provides no support for his contention (Pet. 19-20) that individuals have a greater privacy interest in IP-address records than, for example, in the financial information contained in the "checks, deposit slips, * * * financial statements, and * * * monthly statements" the government acquired in Miller. 425 U.S. at 438. Although the records in Miller were "copies of personal records that were made available to the banks for a limited purpose," this Court nevertheless concluded that no Fourth Amendment search had occurred because the records "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." Id. at 442. That analysis applies with even greater force in this case because, unlike in Miller, the records at issue here are not even copies of documents that petitioner submitted to the email provider, and the government did not require the provider to keep those records. See ibid.

Petitioner's objection flows from the ability of law-enforcement officers to infer from Microsoft's records that petitioner used a computer in a particular location at particular points in time. But "an inference is not a search." Kyllo, 533 U.S. at 33 n.4. Law-enforcement investigators regularly deduce facts about a person's movements or conduct from information gleaned from third parties. Indeed, that is a central feature of criminal investigations. See Donaldson v. United States, 400 U.S. 517, 522 (1971) (explaining that the lack of Fourth Amendment protection for third-party business records was "settled long ago"); id. at 537 (Douglas, J., concurring) ("There is no right to be free from incrimination by the records or testimony of others."). For example, law-enforcement officers can infer from an eyewitness statement that a suspect was in a particular location at a particular time, from a credit-card slip that she regularly dines at a certain restaurant and was there at a specific time, and from a key-card entry log her routine hours at a gym. But merely because facts about a person can be deduced from records or other information in the possession of third parties does not make the acquisition of that information a Fourth Amendment search of the person.

Petitioner points out (Pet. 15) that "the government used the IP login history to locate [petitioner] in his home." But the pen-register records in Smith likewise allowed for the inference

that the defendant was present in his home when he placed telephone calls, and the Court nevertheless concluded that no Fourth Amendment search had occurred. As the Smith Court explained, "[r]egardless of his location, [the defendant] had to convey [information] to the telephone company in precisely the same way if he wished to complete his call," and "[t]he fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference" under the Fourth Amendment. 442 U.S. at 743; see Pet. App. A3 (observing that petitioner's "argument is foreclosed by Smith, in which government officials sought information that they knew was connected to the defendant's home, and in which the Court explicitly rejected an argument identical to [petitioner's]").

Petitioner suggests (Pet. 10-23) that the Fourth Amendment principles recognized in Smith and Miller should not apply to new technologies. Although petitioner relies (Pet. 14, 16-17) on Jones and Riley v. California, 134 S. Ct. 2473 (2014), those decisions did not address -- much less disavow -- this Court's precedents recognizing that an individual does not have a Fourth Amendment interest in a third party's records pertaining to him or in information that he voluntarily conveys to third parties. In Jones, the Court held that the warrantless installation and use of a GPS tracking device on a vehicle to continuously monitor its movements over the course of 28 days constituted a Fourth Amendment

search. 565 U.S. at 402-404. In reaching that conclusion, the Court relied on the fact that the government had "physically intrud[ed] on a constitutionally protected area" -- the suspect's automobile -- to attach the device. Id. at 407 n.3. In this case, by contrast, petitioner does not contend that any such physical occupation occurred. Because the Court in Jones concluded that the attachment of the device constituted "a classic trespassory search," id. at 412, it did not reach the Katz inquiry or hold that tracking a person's vehicle on public streets violates a reasonable expectation of privacy, which would represent a significant qualification of the Court's prior holding in United States v. Knotts, 460 U.S. 276, 281-282 (1983). See Jones, 565 U.S. at 411-413.

This Court's decision in Riley likewise does not aid petitioner's argument. Riley held that a law-enforcement officer generally must obtain a warrant to search the contents of a cell phone found on an arrestee. 134 S. Ct. at 2485. No question existed in Riley that the review of the contents of a cell phone constitutes a Fourth Amendment search; the question was whether that search fell within the traditional search-incident-to-arrest exception to the warrant requirement. See id. at 2482 ("The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest."); see also id. at 2489 n.1 (noting that "[b]ecause the United States and California agree that these

cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances"). Riley thus presented no occasion for this Court to reconsider its longstanding view that an individual has no Fourth Amendment interest in records pertaining to the individual that are created by third parties or in information he voluntarily conveys to third parties.

Even putting aside the specific holdings of Jones and Riley, the broader privacy concerns raised in those cases (and discussed in the concurrences by Justice Alito and Justice Sotomayor in Jones, see 565 U.S. at 414-419 (Sotomayor, J., concurring); id. at 427-431 (Alito, J., concurring in the judgment)) do not justify creating a novel Fourth Amendment rule here. The GPS tracking device in Jones allowed law-enforcement officers to use "signals from multiple satellites" to continuously track the movements of the defendant's vehicle over the course of 28 days, accurate to "within 50 to 100 feet." Id. at 403 (majority opinion). The information the government acquired in this case, by contrast, consisted only of records indicating that a computer using a particular IP address had been used to log in to petitioner's Hotmail account at particular times. See Pet. App. A4. Although those records supported an inference that petitioner had accessed his email account at certain times from work and home, "[t]he

government received no information about how he got from home to work, how long he stayed at either place, or where he was when he was not at home or work." Ibid. "On days when [petitioner] did not log in, the government had no idea where he was." Ibid. And although Microsoft's records contained IP-address information for a 73-day period, id. at A2, the records contained fewer than two IP-address entries per day on average. See D. Ct. Doc. 162-1, at 6-8; see also Pet. 13. This case thus presents no occasion to consider the legal implications of technology capable of "secretly monitor[ing] and catalog[ing] every single movement" an individual makes continuously "for a very long period." Jones, 565 U.S. at 430 (Alito, J., concurring in the judgment); see id. at 415-416 (Sotomayor, J., concurring); see also Pet. App. A4 (stating that petitioner's attempt to liken IP-address records to GPS records "is unhelpful exaggeration").

Likewise, this case does not touch on a central concern in Riley: that cell phones may contain "vast quantities of personal information" that could be used to discern "[t]he sum of an individual's private life," including information about the user's health, family, religion, finances, political and sexual preferences, and shopping habits, as well as GPS records of the user's "specific movements down to the minute, not only around town but also within a particular building." 134 S. Ct. at 2485, 2489, 2490. Even if the same logic applied to email accounts, the

Microsoft records obtained in this case revealed only that petitioner or someone using his email account used certain IP addresses to access that account. They did not (and could not) reveal any information stored in petitioner's email account or permit law-enforcement officers to learn the sort of detailed personal facts that the Court identified in Riley. See Pet. App. B4 (observing that the records disclosed in this case "contained no information concerning the contents of any of [petitioner's] communications").

Petitioner essentially seeks a rule that he has a personal Fourth Amendment interest in the record of his transaction with a business from which his location can be approximately inferred. No recognized Fourth Amendment doctrine supports that contention.[2] The court of appeals therefore correctly held that under this Court's precedents, petitioner has no valid Fourth Amendment interest in records of IP addresses he used to access his Hotmail account created by Microsoft for its own business purposes.

---

[2] Petitioner cites (Pet. 18) a variety of cases that did not involve the third-party doctrine to support his contention that privacy interests may survive even when "[i]nformation [is] in the hands of a third party." None of those cases involved business records created by a third party based on information voluntarily conveyed to the business. For example, Ferguson v. City of Charleston, 532 U.S. 67 (2001), involved urine tests conducted by state hospital staff that "were indisputably searches within the meaning of the Fourth Amendment." Id. at 76. The other cited cases are equally inapposite.

b. Even if petitioner could establish that he has a novel Fourth Amendment interest in the records created and held by Microsoft, the government's acquisition of those records was reasonable and therefore complied with the Fourth Amendment.

"As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'" Maryland v. King, 133 S. Ct. 1958, 1969 (2013) (citation omitted). A "warrant is not required to establish the reasonableness of all government searches; and when a warrant is not required (and the Warrant Clause therefore not applicable), probable cause is not invariably required either." Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995). 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). In addition, in a case that challenges a federal statute under the Fourth Amendment, this Court applies a "strong presumption of constitutionality" to the statute, "especially when it turns on what is 'reasonable'" within the meaning of the Fourth Amendment. United States v. Watson, 423 U.S. 411, 416 (1976) (citation omitted). In light of those principles, even if the acquisition of Microsoft's IP-address records pertaining to petitioner's email logins qualifies as a Fourth Amendment search, that acquisition would be

constitutionally reasonable. That follows for two independently sufficient reasons.

First, as discussed above, this Court has held 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 (reaffirming the "traditional distinction between a search warrant and a subpoena"); see also Oklahoma Press Publ'g Co., 327 U.S. at 209. Rather, as the Court explained in Miller, the Fourth Amendment allows the government to use subpoenas to require the production of "relevant" business records and papers. Miller, 425 U.S. at 445-446 (citation omitted). Such subpoenas are not subject to the same requirements as a search warrant. See ibid. And it is established law that "a person inculpated by materials sought by a subpoena issued to a third party" cannot invoke his own Fourth Amendment rights to object to the production of records by that third-party subpoena recipient. SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 742 (1984). It follows that the SCA procedure -- which specifically contemplates that the government may use an administrative subpoena to obtain IP-address records that belong not to individual subscribers but rather to email providers -- is constitutionally reasonable. Cf. Jones, 565 U.S. at 429-430 (Alito, J., concurring in the judgment) ("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.").

Second, traditional standards of Fourth Amendment reasonableness independently confirm that a subpoena is a reasonable mechanism for obtaining an email provider's IP-address records. 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 and hold that an individual can assert a Fourth Amendment interest in records created by a third party that pertain to a transaction he engaged in with the third party, petitioner could at most assert only a diminished expectation of privacy in those records. That is a factor that this Court has said "may render a warrantless search or seizure reasonable." King, 133 S. Ct. at 1969 (citation omitted). And any invasion of petitioner's assumed privacy interest was minimal, given the limited nature of the location information that could be inferred from the IP-address records at issue here.

On the other side of the reasonableness balance, the government has a compelling interest in obtaining IP-address records using a subpoena, rather than a warrant, because, like other investigative techniques that involve seeking information from third parties about a crime, 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." United States v. Davis, 785 F.3d 498, 518 (11th Cir.) (en banc) (discussing this issue in the context of cell-cite location records), cert. denied, 136 S. Ct. 479 (2015). Society has a strong interest in both promptly apprehending criminals and exonerating innocent suspects as early as possible during an investigation. See King, 133 S. Ct. at 1974; United States v. Salerno, 481 U.S. 739, 750-751 (1987). In short, "a traditional balancing of interests amply supports the reasonableness of" the government's decision to use the subpoena mechanism in the SCA to obtain Microsoft's IP-address records. Davis, 785 F.3d at 518.

2. The courts of appeals that have considered the issue have uniformly found that individuals possess no Fourth Amendment privacy interest in IP addresses conveyed to third-party service providers. See Christie, 624 F.3d at 573-574 (3d Cir.); United States v. Beckett, 369 Fed. Appx. 52, 56 (11th Cir. 2010) (per curiam); Forrester, 512 F.3d at 510 (9th Cir.); United States v. Perrine, 518 F.3d 1196, 1204-1205 (10th Cir. 2008); Pet. App. A2. Petitioner accordingly cannot and does not contend that the courts of appeals are divided on that question. Instead, petitioner argues (Pet. 9, 22) that the Court should grant the petition for a writ of certiorari to review an alleged circuit split regarding "whether the third-party doctrine is still applicable today." But

that alleged circuit split does not exist, and even if it did, petitioner's case would be a poor vehicle for resolving it.

a. Petitioner contends (Pet. 9-10, 17-18) that the courts of appeals are divided on whether the third-party doctrine applies to historical "cell-site" records, which show the cell towers with which a cell phone has connected while in use. That is incorrect.

The Fourth, Fifth, Sixth, and Eleventh Circuits have each held that the government's acquisition of cellular-service providers' cell-site records pursuant to courts orders authorized by the SCA does not violate the Fourth Amendment. See United States v. Graham, 824 F.3d 421, 425-438 (4th Cir. 2016) (en banc), petitions for cert. pending, No. 16-6308 (filed Sept. 26, 2016), and No. 16-6694 (filed Oct. 27, 2016); United States v. Carpenter, 819 F.3d 880, 886-890 (6th Cir. 2016), petition for cert. pending, No. 16-402 (filed Sept. 26, 2016); Davis, 785 F.3d at 506-516 (11th Cir.); In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 609-615 (5th Cir. 2013) (Fifth Circuit In re Application). Petitioner contends (Pet. 9) that those decisions conflict with the Third Circuit's decision in In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304 (2010) (Third Circuit In re Application).[3] But the Third

[3] Petitioner also cites (Pet. 18) Tracey v. State, 152 So. 3d 504 (Fla. 2014), and Zanders v. State, 58 N.E.3d 254 (Ind. Ct. App.), vacated and transfer granted, 62 N.E.3d 1202 (Ind.

Circuit addressed only the statutory standard for obtaining cell-site records under the SCA, id. at 308-319, and the court expressly "h[eld] that [historical cell-site data] from cell phone calls is obtainable under" an order issued in compliance with 18 U.S.C. 2703(d), which "does not require the traditional probable cause determination." Id. at 313.

b. In any event, this case does not involve cell-site records and so would not provide an appropriate vehicle to resolve any disagreement among lower courts about whether the Fourth Amendment permits the government to acquire those records pursuant to an SCA order. Indeed, just eight days after the Third Circuit issued its opinion in Third Circuit In re Application, which petitioner describes (Pet. 18) as "conclud[ing] that a [cell-phone] user does not voluntarily convey location information," the Third Circuit held that "no reasonable expectation of privacy exists in an IP address" because computer users "voluntarily turn[] over [that information] in order to direct the third party's servers."

2016). But the Supreme Court of Florida's decision in Tracey considered only whether the use of prospective, "real time cell site location information" to continuously monitor an individual's movements requires a warrant under the Fourth Amendment, 152 So. 3d at 515 (emphasis added); see id. at 525-526, and the court made clear that its holding did not encompass historical cell-site records like those at issue in the decisions petitioner contends are in conflict. Id. at 508, 515, 516, 526. Petitioner's reliance on Zanders likewise is misplaced because that decision was recently vacated when the Supreme Court of Indiana granted discretionary review.

Christie, 624 F.3d at 574 (quoting Forrester, 512 F.3d at 510). Petitioner therefore errs in suggesting (Pet. 22) that this case provides an "ideal opportunity" to resolve an alleged conflict on whether cell-site records implicate the Fourth Amendment.

3. Even if the question presented warranted this Court's review, this case would be an unsuitable vehicle to address it because the good-faith exception to the exclusionary rule provides an independent basis for affirming the district court's denial of petitioner's suppression motion. See Gov't C.A. Br. 26-27 (arguing that the good-faith exception applies).

As this Court has explained, the exclusionary rule is a "judicially created remedy" that is "designed to deter police misconduct rather than to punish the errors of judges and magistrates." United States v. Leon, 468 U.S. 897, 906, 916 (1984) (citation omitted). "As with any remedial device, application of the exclusionary rule properly has been restricted to those situations in which its remedial purpose is effectively advanced." Illinois v. Krull, 480 U.S. 340, 347 (1987). The rule therefore does not apply "where [an] officer's conduct is objectively reasonable" because suppression "cannot be expected, and should not be applied, to deter objectively reasonable law enforcement activity." Leon, 468 U.S. at 919. For that reason, "evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be

charged with knowledge, that the search was unconstitutional under the Fourth Amendment." Ibid. (citation omitted).

This Court has held that the good-faith exception applies to "officer[s] acting in objectively reasonable reliance on a statute," later deemed unconstitutional, that authorizes warrantless administrative searches. Krull, 480 U.S. at 349; see id. at 342. It follows a fortiori that officers act reasonably in relying on a statute that recognizes that the government may acquire a third party's business records pursuant to a subpoena. In addition, no binding appellate decision (or holding of any circuit) has suggested, much less held, that the SCA is unconstitutional as applied to IP-address records. Given that, officers were entitled to rely on the presumption that acts of Congress are constitutional. Cf. Davis v. United States, 564 U.S. 229, 241 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule."). Thus, even if the government's acquisition of the IP-address records constituted a search in violation of the Fourth Amendment, the good-faith exception would apply. Because the district court therefore correctly denied the motion to suppress and petitioner would not obtain relief even if this Court were to rule in his favor on the Fourth Amendment question, review of that question is not warranted in this case.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

NOEL J. FRANCISCO
Acting Solicitor General

KENNETH A. BLANCO
Acting Assistant Attorney General

JENNY C. ELLICKSON
Attorney

FEBRUARY 2017