No. _____

IN THE SUPREME COURT OF THE UNITED STATES
OCTOBER TERM, 2016

FRANK CAIRA,

PETITIONER,

vs.

UNITED STATES OF AMERICA,

RESPONDENT.

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

HANNAH VALDEZ GARST
Law Offices of Hannah Garst
121 S. Wilke Rd.
Suite 301
Arlington Heights, IL 60005
(773)248-6504
hannahgarst@garstlaw.com

COUNSEL FOR PETITIONER

QUESTION PRESENTED

Whether this Court should resolve a split of authority among the courts by rejecting the Seventh Circuit's reasoning in *United States v. Caira*, which holds that individuals have no reasonable expectation of privacy in information held by a third party.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules

No. _____

IN THE SUPREME COURT OF THE UNITED STATES
OCTOBER TERM, 2016

FRANK CAIRA,

PETITIONER,

vs.

UNITED STATES OF AMERICA,

RESPONDENT.

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

Petitioner Frank Caira respectfully petitions for a writ of certiorari to review the judgment and opinion of the United States Court of Appeals for the Seventh Circuit, which was entered in the above-entitled case on August 17, 2016.

OPINION BELOW

The opinion of the United States Court of Appeals for the Seventh Circuit, entitled *United States v. Caira*, No. 14-1003, slip opinion, decided August 17, 2016, is reported at 2016 U.S. App. LEXIS 15098 (7th Cir. 2016) and included in the appendix attached hereto at Appendix A: 1-4.

JURISDICTION

The U.S. District Court for the Northern District of Illinois originally had jurisdiction pursuant to 18 U.S.C. § 3231, which provides exclusive jurisdiction of offenses against the United States. Thereafter, the Petitioner timely appealed his convictions and sentences to the United States Court of Appeals for the Seventh Circuit pursuant to 28 U.S.C. § 1291. The jurisdiction of this Court is invoked pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution states:

> 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 person or things to be seized.

The Stored Communications Act, 18 U.S.C. § 2703, states in pertinent part:

> (c) Records Concerning Electronic Communication Service or Remote Computing Service.---(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,

> 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).

STATEMENT OF THE CASE

Following a guilty plea in the United States District Court for the Northern District of Illinois, the court found Mr. Caira guilty of conspiracy to distribute a controlled substance, in violation of 21 U.S.C. § 846, and conspiracy to manufacture and possession with intent to distribute a controlled substance, in violation of 21 U.S.C. §§ 841(a)(1) & 846. In the plea agreement, Mr. Caira reserved the right, pursuant to Fed. R. Crim. Proc. 11(a)(2), to appeal the district court's denial of his motion to suppress evidence obtained through the use of administrative subpoenas. The district court sentenced Mr. Caira to 300 months' imprisonment. The Seventh Circuit affirmed Mr. Caira's conviction and concluded that the government's use of administrative subpoenas did not amount to a search under the Fourth Amendment, because Mr. Caira voluntarily shared his IP address with a third party and therefore had no reasonable expectation of privacy. Appendix A: 2-4.

When a device accesses the internet, it uses a unique numerical address called an Internet Protocol ("IP") address to identify itself to other computers. *Nat'l*

Cable & Telecomm. Ass'n v. Brand X Internet Svcs., 545 U.S. 967, 987, n.1 (2005). Simply, an IP address is a series of four (4) numbers separated by periods, and each of the four (4) numbers is a whole number between zero (0) and two hundred fifty five (255). Each time individuals access the Internet, the device is assigned an IP address. Each Internet Service Provider ("ISP") is associated with a particular block of IP addresses for use by that ISP's customers or subscribers. *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 120 (E.D. Va. 2011). The ISP logs the date, time, and duration of the internet session for each IP address and can identify the user of that IP address for a particular session from these records.

Between July 9 and September 17, 2008, an unknown individual emailed a Drug Enforcement Administration (DEA) controlled website based in Hanoi, Vietnam, purportedly in an effort to purchase and import Sassafras Oil. Sassafras Oil is primarily composed of Safrole, a list I chemical under 21 U.S.C. § 802(34)(Q). The emails were sent from gslabs@hotmail.com which was registered in the name Jeff Hurst. These emails were either unsigned or signed only with the name "Steve." Appendix B: 5.

The emails between gslabs@hotmail.com and an undercover agent posing as "Miss Tran Thuy" discussed the price for 55 gallons of Sassafras Oil and the cost to ship the oil to an address in Chicago, Illinois. At the agent's request, "Steve" also provided a telephone number, so he could be contacted about the status of the delivery. Another agent identifying himself as "Todd" attempted to contact "Steve"

at the above number but was only able to leave voicemails. Additional emails concerned the payment arrangements and "Todd's" contact information.

Registration with the Attorney General is required to import any list 1 chemical into the United States. 21 U.S.C. § 957(a). Sassafras Oil is a list 1 chemical, because it is primarily composed of Safrole. Although Safrole is used to manufacture MDMA ("ecstasy"), it is also an important raw material in pesticides and as a fragrance in household products such as floor waxes, polishes, soaps, detergents and cleaning agents. DEA records indicated that neither Jeff Hurst nor GS Labs were registered to import Safrole, nor was Chicago address associated with anyone who was registered to import Safrole.

In an effort to locate the user of the Hotmail address, on September 2, 2008, the DEA issued an administrative subpoena[1] to Microsoft Corporation requiring the disclosure of "all basic subscriber information, including the subscriber name, address, length of service (including start date) and types of services used including any temporarily assigned network address, Passport.net accounts, means and source of payment (including credit card or bank account number), and the account

[1] The government did not obtain a search warrant or any authorization from a court prior to the issuance of any administrative subpoena. However, twenty-four days after issuing the administrative subpoena, the government obtained a search warrant to obtain subscriber information, transactional information, including IP login history, and emails from the gslabs@hotmail.com. Upon Mr. Caira's motion, the district court quashed the warrant due to government's failure to include material information in the affidavit but later vacated the order after the government indicated that it did not intend to use any of the information obtained from the warrants but instead planned to rely on the administrative subpoenas.

login histories (IP login history) of, the following email account(s): gslabs@hotmail.com."

In response to the subpoena, Microsoft turned over several documents. The first document included basic subscriber information, which included first and last name, state, zip code, country, IP address from which the account was registered, and the date the account was created. This IP address was linked to Mr. Caira's employer Northwestern University. Microsoft also turned over the entire IP login history for gslabs@hotmail.com, which included a series of 114 logins and corresponding IP addresses (spanning 73 days), and date and times. From this information, the government discovered that 24.15.180.222 was an IP address frequently used to access gslabs@hotmail.com.

The government thereafter issued a subpoena to Comcast IP Services, the owner of IP address 24.15.180.222, and requested that Comcast disclose "records related to 24.15.180.222 including any and all email addresses associated with that IP address; a) customer name and other user name(s); b) addresses; c) records of session times and durations; d) length of service (including start date) and types of service used; 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 credit card or bank account numbers)." Appendix B: 5-6.

In response to the subpoena, Comcast turned over the subscriber information for IP address 24.15.180.222. This information included the subscriber name, which

turned out to be Mr. Caira's wife, the home address, telephone number, type of service, account number, creation date, email users IDs, current IP address and method of payment. Agents determined that Mr. Caira worked at Northwestern University, lived at the address disclosed by Comcast, and used this information to conduct further investigation that resulted in trash pulls from the residence. Appendix B: 5-6.

Mr. Caira filed a motion to suppress evidence and asserted that the government's actions amounted to a search under the Fourth Amendment, because he had a reasonable expectation of privacy in the detailed history of IP addresses used to log into his email address. The motion noted that Mr. Caira had a subjective expectation of privacy not in the basic subscriber information but rather in the detailed history of locations and every IP address which was used to access his personal e-mail account. Appendix B: 5-10. Mr. Caira further argued that although the Stored Communications Act ("SCA"), 18 U.S.C. § 2703, authorizes the use of administrative subpoenas to obtain basic subscriber information, the SCA does not authorize the government to obtain a detailed history of every IP address used to access the email account and the dates when these addresses were used.

The government opposed the motion on the grounds that (1) Mr. Caira did not have a reasonable expectation of privacy in a third party's records regarding his email account or in the records collecting the IP addresses that he used to access his e-mail; and (2) the SCA authorized the government to obtain the information it obtained here, emphasizing that 18 U.S.C. § 2703(c)(2) authorizes administrative

subpoenas to obtain (c) "…records of session times and durations and (D) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;..."

The district court denied Mr. Caira's motion to suppress and ruled that Mr. Caira did not have a reasonable expectation of privacy in the subscriber information provided to an internet provider (a third party), including the detailed history of locations from which he accessed his personal e-mail account. Appendix B: 6-9. It also concluded that the materials authorized for disclosure by 18 U.S.C. § 2703(c) were "precisely the type obtained here." Appendix B: 8.

The Seventh Circuit, who had jurisdiction pursuant to 28 U.S.C. § 3231, agreed with the district court and affirmed Mr. Caira's conviction. Appendix A: 1-4. The Seventh Circuit concluded that *United States v. Miller*, 425 U.S. 435 (1976), and *Smith v. Maryland*, 442 U.S. 735 (1979), controlled the outcome because Mr. Caira voluntarily shared his IP address with a third party. Appendix A: 2-4 Therefore, the government's use of administrative subpoenas did not amount to a search under the Fourth Amendment, and Mr. Caira had no reasonable expectation of privacy. Appendix A: 4. The Seventh Circuit concluded that Mr. Caira had no reasonable expectation of privacy based on the third party doctrine and did not address his argument that the Stored Communications Act would not apply if he had a reasonable expectation of privacy under the *Katz* test.

REASONS FOR GRANTING THE WRIT

This petition arises out of an unresolved issue that affects virtually every person in the United States who uses an email address or the internet. Specifically, this petition involves the Fourth Amendment implications of the government's use of new technology to determine a person's location. This Court has historically required a warrant to monitor an object once it entered the home, *United States v. Karo*, 468 U.S. 705, 714-16 (1984), obtain information about locations of people and objects within a home, *Kyllo v. United States*, 533 U.S. 27, 29-30 (2001), and track a person's location by attaching a GPS device to his vehicle over an extended period of time, *United States v. Jones*, 132 S. Ct. 945, 949-56 (2012).

In the context of current technology, the courts have been increasingly reliant on the third party doctrine to uphold warrantless searches and defeat Fourth Amendment claims. However, the federal courts of appeals have not uniformly applied the third party doctrine. A circuit split exists on whether the third-party doctrine is still applicable today. The Third Circuit has held that the third party doctrine does not apply to CSLI because individuals do not voluntarily convey their locational data in any meaningful sense. *In re United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 317-18 (3d Cir. 2010) ("*In re Application (Third Circuit)*"); *see also Jones*, 132 S. Ct. at 957 (Sotomayor, J. concurring); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). However, the 4th, 5th, and 7th, and 11th Circuits continue to apply *Smith* and *Miller* and have concluded that there is no subjective or objective reasonable

expectation of privacy in a third-party's business record. Appendix A: 2-4; *United States v. Graham*, 824 F.3d 421, 427-28 (4th Cir. 2016) (en banc); *United States v. Davis*, 785 F.3d 498, 511 (11th Cir. 2015); *see In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 611-15 (5th Cir. 2013) ("*In re Application (Fifth Circuit)*").

I. This case presents the question of whether this Court's pre-internet precedents apply to the new technologies that aggregate location data over time.

This case presents the unsettled issue of the privacy and property interests in the collection of location data over a period of time as well as the continued viability of the third party doctrine in a world where unlimited amounts of private information are controlled by third parties. The Fourth Amendment unequivocally protects individuals against intrusion by the government on their reasonable expectations of privacy. *See, e.g., Bond v. United States*, 529 U.S. 334, 340 (2000) (citing *Smith*, 442 U.S. at 740, in turn quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). The Supreme Court has recognized that the government may not exploit evolving technologies to "erode the privacy guaranteed by the Fourth Amendment." *Kyllo*, 533 U.S. at 34. The government, if it employs technology to learn information that would be available otherwise only by means of a warrant, has engaged in a search in violation of the Fourth Amendment. *Karo*, 468 U.S. at 715–16.

Today, the use of the internet, email, and cell phones has become "so pervasive that some persons may consider [it] to be [an] essential means or

necessary instrument [ ] for self-expression, even self-identification." *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010). In order to use this technology, users rely on third party companies who provide these services. Despite the inclusion of this third party, over 80% of people consider "[d]etails of [their] physical location over time" to be "sensitive." Pew Research Ctr., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, 32, 34 (Nov. 12, 2014) (Available at*: http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/).* Privacy of location information while utilizing current technology falls squarely within the societal expectation that people should be protected from warrantless searches and seizures and locational information should remain private. This is especially true when it comes to the home. "[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable." *Karo*, 468 U.S. at 714-15 (collecting cases).

Technology companies obtain data each time a person accesses the internet, including each time you send or receive email. The data includes logs that detail the time, date, and location of a user, how a user came to find a product, and what a user viewed while using the internet. Alexandra D. Vesalga, *Location, Location, Location: Updating the Elec. Communications Privacy Act to Protect Geological Data*, 42 Golden Gate U. L. Rev. 459, 459-60 (2013). "Geolocational data---data that pinpoints a user's location---is among the most useful, vital, and coveted data for technology companies, as it allows a web service to make relevant suggestions based

on a user's real-time location and improves the relevance of targeted online advertising." *Id.* at 460.

Location information in the hands of these third parties have created privacy concerns for individual citizens. Mr. Caira's case is not an isolated or occasional concern. Law enforcement is requesting staggering volumes of information from Internet Service Providers. For example, Comcast reported that in the first half of 2016, it received 10,819 criminal requests.[2] *Available at:* http://corporate.comcast.com/images/Sixth-Comcast-Transparency-Report.pdf (last visited 10/21/16). Of these requests, 8,414 were based on administrative subpoenas[3], 1,651 court orders, and 754 warrants. *Id.* The government is actively using its subpoena power, which requires no judicial oversight, to gain access to information that may be protected under the Fourth Amendment.

Following *Smith* and *Miller*, several court have held that e-mail and Internet users have no expectation of privacy in in their IP address. S*ee United States v. Suing*, 712 F.3d 1209, 1213 (8th Cir. 2013) (shared IP address on peer to peer network); *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (IP addresses are voluntarily conveyed to third party, including ISPs); *United States v. Forrester,* 512 F.3d 500, 510 (9th Cir. 2008) (same). The Ninth Circuit found the government's acquisition of this information constitutionally indistinguishable from the use of a

[2] National Security Requests are not included in these numbers.
[3] Comcast defined subpoenas as frequently seeking identification of a customer account based on a telephone number or IP address assigned to the account. The subpoenas are usually issued by law enforcement or a prosecuting attorney.

pen register that the Court approved in *Smith*, in part because "e-mail and Internet users, like the telephone users in *Smith*, rely on third-party equipment in order to engage in communication," and IP addresses "are voluntarily turned over in order to direct the third party's servers." *Id.* at 510. Of course, computer users do actively choose to share some of the information discussed in the above cases, like the "to" address in an email and the subscriber information conveyed when signing up for Internet service. But users do not "actively choose to share" other pieces of information, like an IP address or the amount of data transmitted to their account. Internet service providers automatically generate that information. *See Christie*, 624 F.3d at 563; *cf. Forrester,* 512 F.3d at 511.

A. The collection of private and personal data in this digital age requires a fresh look at *Smith* and *Miller*, which were based on pre-digital technology that are virtually non-existent in today's world.

Here, as a matter of routine, the government used an administrative subpoena to obtain locational information at 114 different points in time over a period of 73 days. The lower courts need guidance on how to handle locational data that is being collected without any judicial oversight. *Smith* and *Miller* were decided in 1979 and 1976, respectively. The third-party collection of information in the late 70s is light years away from the vast quantity of private information now collected on a second-by-second basis.

Furthermore,"[i]ntrinsic to the [third party] doctrine is an assumption that the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy." *Graham*, 824 F.3d

at 436. But in the context of GPS, this Court has agreed that the use of long-term monitoring impinges on the expectation of privacy. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring), at 964 (Alito, J., concurring).

In the CSLI context, Justice Sotomayor explained, electronic location tracking implicates the Fourth Amendment because "it generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955. The Supreme Court also recently stated that cell phone locational data raises particularly acute privacy concerns because it "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014) (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)). This same logic should be applied to all facets of current technology involving the internet and email. Long-term location information disclosed in an extended IP login history provides detailed information and reveals comprehensive and specific details of a person's life. IP addresses are analogous to CSLI information, because an IP login history allows the government to locate a person at private locations at specific points in time.

The IP login history is more invasive than GPS and equally invasive as CSLI data, because IP addresses provide meaningful information about a person's actual physical location as well as the network and even the specific machine being used. *See Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 409-10 (2d Cir. 2004) (IP

addresses identify the computer's location). Here, the violation of privacy is more obvious, because the government used the IP login history to locate Mr. Caira in his home on 70 occasions. When it issued the administrative subpoena, the government did not know the owner of gslabs@hotmail.com or his location. His IP address was critical information, because it led the government to Mr. Caira and his home. The government used technology not available to the general public to essentially reach through Mr. Caira's email address into his home, a protected space.

"The sanctity of the home is a central concern of the Fourth Amendment." *United States v. Etchin*, 614 F.3d 726, 733 (7th Cir. 2010). It is therefore "a basic principle of Fourth Amendment law that searches and seizures inside a home without a warrant are presumptively unreasonable." *Payton v. New York*, 445 U.S. 573, 586 (1980) (internal quotation marks omitted). "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Silverman v. United States*, 365 U.S. 505, 511 (1961).

A fresh look at *Smith* and *Miller* would give this Court an opportunity to consider the third party doctrine in light of current and future technology. It would provide guidance to courts who are struggling to apply Fourth Amendment principles to the vast quantity of information being sought by the government, oftentimes through a procedure that requires little, if any, judicial oversight.

B. This Court should grant certiorari to reconsider the reasonable expectation of privacy and third-party principles from *Katz*, *Smith*, and *Miller*.

Both the Fourth and Seventh Circuits recently noted that this Court may decide to revisit the third-party doctrine. Appendix A: 4; *Graham*, 824 F.3d at 437. In addition, in *Jones*, Justice Sotomayor wrote that the third-party doctrine "'is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.'" Appendix A: 4 (quoting *Jones,* 132 S. Ct. at 957). As the Fourth Circuit stated, "although the Court formulated the third-party doctrine as an articulation of the reasonable-expectation-of-privacy inquiry, it increasingly feels like an exception. A per se rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy." *Graham*, 824 F.3d at 437 (emphasis in original). But Justice Sotomayor articulated that "tailoring the *Fourth Amendment* to 'the digital age' would require the Supreme Court itself to 'reconsider' the third-party doctrine." *Id.* (quoting *Jones*, 132 S. Ct. at 957). Honing in on subjective expectations of privacy, Justice Sotomayor doubted "people would accept without complaint the warrantless disclosure" of information to the government from their ISPs like URLs they visit or the email addresses with which they correspond. *Jones*, 132 S. Ct. at 957.

Five Justices have "expressed the view that technology has changed the constitutional calculus by dramatically increasing the amount and precision of data that the government can easily collect." Appendix A: 4 (citing *Jones*, 132 S. Ct. at

955-56 (Sotomajor, J., concurring); 964 (Alito, J., concurring)). The break-neck speed of technology, along with future advances, has highlighted the weakness of the *Katz* test that is based on a subjective and objective test of the reasonable expectation of privacy. Justice Harlan in *Kyllo* noted that the "*Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable." *Kyllo*, 533 U.S. at 34; *see also Katz*, 389 U.S. at 361 (Harlan, J., concurring). *Kyllo* also rejected a "mechanical interpretation of the Fourth Amendment" in the face of "advancing technology." *Kyllo*, 533 U.S. at 35.

The Court in *Jones*, however, relied on a more narrow ground to find a Fourth Amendment violation and never reached the issue of the third-party exception to the reasonable expectation of privacy test. Again in *Riley*, despite the government's argument that *Smith* permitted it to inspect call logs on a cell phone, this Court decided it need not address whether the inspection amounted to a Fourth Amendment search. *Riley*, 134 S. Ct. at 2492-93. The Court did note that information on one's cell phone call log was not analogous to the limited information available from a pen register. *Id.* at 2493.

This Court has yet to decide whether the mere use of current technology constitutes voluntary conveyance of data and thus not afforded Fourth Amendment protections. In the context of CSLI, the courts are split over whether people knowingly and voluntarily expose their movements to their cellular service providers. The Fourth, Fifth, Sixth, and Eleventh Circuits have decided that one's

use of a cell phone amounts to voluntary exposure of one's movement, thus the third party doctrine applies, while the Third Circuit, the Florida Supreme Court, and the Indiana Court of Appeals have concluded that a user does not voluntarily convey location information, thus the doctrine does not apply. *See Graham*, 824 F.3d at 427-28; *In re Application (Fifth Circuit)*, 724 F.3d at 613; *Davis*, 785 F.3d at 511; *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016); *In re Application (Third Circuit)*, 620 F.3d at 317; *Tracey v. State*, 152 So. 3d 504, 522-26 (Fl. 2014); *Zanders v. State*, 58 N.E.3d 254, 263 (Ind. Ct. App. 2016); *see also Warshak*, 631 F.3d at 287-88 (*Smith* and *Miller* do not endorse a blind application of the third party doctrine for information where a reasonable expectation of privacy exists but is recorded by a third party through an accident of technology).

In the digital age, telephone and cable companies, internet service providers, and app developers enable private communications. Much of the digital communication is tailored to the limited audience chosen by the user. Information in the hands of a third party is not categorically excluded from protection under the Fourth Amendment. *Ferguson v. City of Charleston*, 121 S. Ct. 1281, 1288 (2001); *see, e.g., United States v. Jacobsen*, 466 U.S. 109, 114 (1984); *Stoner v. California*, 376 U.S. 483, 487-88, 490 (1964). The third-party doctrine denies *Fourth Amendment* protection only for information that has been "voluntarily conveyed" by an individual to a third party. *Graham*, 824 F.3d at 435, 442 (Wynn, J., dissent); *see Smith,* 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company . . . ."); *id.* at 745 ("[P]etitioner

voluntarily conveyed to [the phone company] information that it had facilities for recording . . . .")*; Miller,* 425 U.S. at 442 ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks . . . ."). Voluntary conveyance means that the person knows he is communicating particular information and completed some act to submit that specific information to a third party. *Smith*, 442 U.S. at 741; *Miller*, 425 U.S. at 442. "The Court never suggested that the simple act of signing up for a bank account, or a phone line, was enough to willingly turn over thousands of pages of personal data." *Graham*, 824 F.3d at 443 (Wynn, J., dissent).

The *location* of the user logging into his email is not comparable to the numerical information affirmatively disclosed by the customer when he pressed each number as he dialed his phone. Logging into his email did not constitute a voluntary conveyance of his locational information. *Smith* does not attempt to address records as to a subscriber's location at the time of calls. Set in 1979, *Smith* involved landline telephones, and this Court could never have remotely contemplated its application to the far different context of IP addresses and locational data. *See Smith,* U.S. at 743 ("Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call.") The Court in *Smith* found that "all subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, *for they see a list of their long-distance (toll) calls on their monthly bills*." 442 U.S. at 742 (emphasis added). Today, this information is not

provided to users, and it is also questionable as to whether the provider would generate it upon the user's request.

Applying *Miller* to today's technology is problematic for the same reasons. Bank customers personally directed their banks to pay or deposit money and in turn, they received a monthly bank statement setting forth each transaction. *Miller*, 425 U.S. at 442. Customers participated in concrete transactions and understood steps the banks would take to complete these transactions. This is not so for email and internet usage; a user's conduct is materially different from the active, deliberate choices made to disclose information that the Court discussed in *Miller*.

Technological advances allow data to be constantly tracked, whether it be through email, cell phone, internet, or other device. The application of the third-party doctrine to locational data "fails to recognize the intrusive nature of this data in comparison with previous technologies." Vesalga, 43 Golden Gate U. L. Rev. at 479. The 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. *See id.* Aside from the postmark, an envelope includes only the information the sender wishes to include. *Id.* A call log reveals only that the person was at a particular location at a certain time and what phone number he or she called. *Id.* IP addresses reveal "a user's precise location or locational movements over a period of time." *Id.*

Although internet and email users may be willing to share data with their ISP for marketing or an improved user experience, it does not mean that they have

relinquished all privacy to warrantless searches by the government. *See id.* "It defies all logic and commonsense to argue that Internet users, who share personal information with trusted websites in exchange for free or improved services should assume that this information may be shared with the government…" without a warrant. *Id.* at 480.

Disclosure of this data is not a choice if people want to use email or the internet. In *Smith*, Justices Marshall and Brennan dissented, noting that it is unacceptable to force people to accept the risk or surveillance or forgo the use of the phone. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting). For most people, this is not a choice; email and internet use is virtually mandatory in nearly every profession. *See* Vesalga, 43 Golden Gate U. L. Rev. at 481. "It is untenable to require that Americans forgo use of the Internet to protect their privacy." *Id.* In *Davis*, Judge Rosenbaum concurred in the outcome but expressed that the third-party doctrine warranted additional consideration and discussion. *See Davis*, 785 F.3d at 525 (Rosenbaum, J. concurring). He stated:

> In our time, unless a person is willing to live 'off the grid,' it is nearly impossible to avoid disclosing the most personal of information to third-party providers on a constant basis, just to navigate daily life. And the thought that the government should be able to access such information without the basic protection that a warrant offers is nothing less than chilling.

Id. "[I]f a new technology permits the government to access information that it previously could not access without a warrant, using techniques not regulated under preexisting rules that predate technology, the effect will be that the Fourth

Amendment matters less and less over time." Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 215 Harv. L. Rev. 476, 527 (2011).

II. This case presents the ideal opportunity to resolve the question of whether the third party doctrine applies to today's technology, because this question has been fully litigated and is supported by a well-developed factual record.

This case provides this Court with the opportunity to revisit and resolve the application of the third party doctrine to current technology. Courts across the country are being faced with considering whether the government's requests for detailed, personal, private information falls within the protections of the Fourth Amendment. Unlike other IP address cases, these issues have been fully briefed and considered in both the district and circuit court. Furthermore, this case involves the government asking for and obtaining data covering 112 days. The administrative subpoenas and IP login history, along with the relevant motion to suppress, are all a part of the well-developed trial record.

In addition, there are no disputes of material fact and no procedural obstacles that would prohibit resolution of the merits of this case. The government never raised any argument in the district court that the good faith exception to the exclusionary rule would apply to this case. Even so, the government's application for a warrant was quashed in the district court due to government's failure to include material information in the affidavit. The district court later vacated the order but only after the government indicated that it did not intend to use any of the information obtained from the warrants and planned to rely exclusively on the administrative subpoenas.

If the third party doctrine does not apply, Mr. Caira's motion to suppress should be granted, and the evidence obtained from the administrative subpoenas suppressed. He should be afforded protection under the Fourth Amendment. Equally important, this Court can reconsider the third party doctrine, as part of the reasonable expectation of privacy test, and its application to the digital age.

CONCLUSION

For the reasons noted herein, Petitioner respectfully prays that a writ of certiorari issue to review the judgment and opinion of the United States Court of Appeals for the Seventh Circuit entered on August 17, 2016.

Respectfully submitted,

HANNAH VALDEZ GARST
Counsel of Record for Petitioner
Law Offices of Hannah Garst
121 S. Wilke Rd.
Suite 301
Arlington Heights, IL 60005
(773)248-6504
hannahgarst@garstlaw.com

APPENDICES:

APPENDIX A

United States v. Caira, No. 14-1003, 2016 U.S. App. LEXIS 15098 (7th Cir. Aug. 17, 2016)

APPENDIX B

United States v. Caira, Case. No. 08-cr-01052. (N.D. Ill. 2012)
Dkt. 188- District Court Order

No. _____

IN THE SUPREME COURT OF THE UNITED STATES
OCTOBER TERM, 2016

FRANK CAIRA,

PETITIONER,

vs.

UNITED STATES OF AMERICA,

RESPONDENT.

PROOF OF SERVICE

I, Hannah Valdez Garst, do swear and declare that on this date, October 31, 2016, as required by Supreme Court Rule 29, I have served the enclosed MOTION FOR LEAVE TO PROCEED *IN FORMA PAUPERIS* and PETITION FOR WRIT OF CERTIORARI on each party to the above proceeding or that party's counsel, and on every other person required to be served, by depositing an envelope containing the above documents in the United States mail properly addressed to each of them and with first-class postage prepaid, or by delivery to a third-party commercial carrier for delivery within 3 calendar days.

The names and addresses of those served are as follows:

Solicitor General of the United States
Rm. 5616
Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530-0001

Stephen Chahn Lee
United States Attorney's Office
N.D. of Illinois, Eastern Division
219 S. Dearborn St., 5th Floor
Chicago, IL 60604

I declare under penalty of perjury that the foregoing is true and correct.

Executed on October 31, 2016

_____
Hannah Valdez Garst
Counsel of Record for Petitioner