No. 16-6761

IN THE
SUPREME COURT OF THE UNITED STATES

FRANK CAIRA,

Petitioner,

vs.

UNITED STATES OF AMERICA,

Respondent.

PETITIONER'S REPLY BRIEF

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Rules

REPLY BRIEF FOR THE PETITIONER

The government failed to recognize the court of appeals are divided on the Question Presented, and the Seventh Circuit's decision rested squarely on its belief that individuals have no reasonable expectation of privacy in information held by a third party. The government urges this Court to deny this petition based on two pre-digital cases decided nearly 40 years ago and conclude that law enforcement may obtain unlimited information possessed by a third party. In light of the vast advances in technology and the quantity of information now held by third parties, the Question Presented is important and the conflict should be resolved without delay. This Court has noted 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," and both the Fourth and Seventh Circuits have recently noted that this Court may revisit this doctrine. *United States v. Jones*, 132 S. Ct. 945, 957 (2012); *United States v. Graham*, 824 F.3d 421, 437 (4th Cir. 2016) (en banc), petitions for cert. pending, No. 16-6308 (filed Sept. 26, 2016) and No. 16-6694 (filed Oct. 27, 2016); *see* Pet. App. A4.

This case presents a uniquely strong vehicle for the Court to resolve the circuit split regarding the application of the third party doctrine to current and future technology. The government failed to raise the good-faith exception to the exclusionary rule in the district court and confirmed this at oral argument. Because this argument was never presented, Petitioner's case provides this Court the opportunity to decide the Question Presented on the merits without analysis of the

good-faith exception. Whether the third party doctrine applies to technology is an issue of great importance affecting nearly every person in the United States.

I. The Government Failed to Recognize the Circuit Split on the Question Presented.

The government incorrectly contends that no circuit split exists on whether the third-party doctrine applies to technology collecting location information. BIO 26-28. The Third Circuit has concluded that a user does not "voluntarily" share one's "location information with a cellular provider in any meaningful way," thus the third-party doctrine does not apply. *In re U.S. for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't,* 620 F.3d 304, 317 (3d Cir. 2010); *see United States v. Smith,* No. 15-180, 2017 U.S. Dist. LEXIS 11910, at *18 (E.D. Pa. Jan. 26, 2017) ("Although other circuits have found that cell phone users do not have a reasonable expectation of privacy in CSLI, I am bound by Third Circuit precedent and therefore cannot conclude that cell phone users do not have a reasonable expectation of privacy in any circumstance."). 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, therefore users have no reasonable expectation of privacy and the third party doctrine applies. *See Graham*, 824 F.3d at 427-28; *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013); *United States v. Davis*, 785 F.3d 498, 511 (2015) (cert. denied, 136 S. Ct. 479 (2015)); *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016) petition for cert. pending, No. 16-402 (filed Sept. 26, 2016). Here, the Seventh Circuit concluded that Petitioner had no reasonable expectation of privacy in the IP

addresses used to log into his email, because he voluntarily shared this information with Microsoft who created and maintained these records. Pet. App. A2-3.

The Seventh Circuit is in conflict with the Third Circuit on whether people voluntarily expose their location information to third parties. Although the Third Circuit has examined this in the context of CSLI, the same analysis applies to the collection of an IP Login History. Just like CSLI, IP Login History is collected and stored by third parties without any active conveyance by the user. 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." Pet. App. A4 (citing *Jones*, 132 S. Ct. at 955-56 (Sotomajor, J., concurring); 964 (Alito, J., concurring)). The Question Presented encompasses whether users have a reasonable expectation of privacy in data collected by third parties. This Court has yet to decide whether the mere use of current technology constitutes a voluntary conveyance of data and thus no Fourth Amendment protections apply.

II. The Question Presented is Important

1. Relying on *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), the government asserts that using a subpoena to acquire records from a third party does not constitute a Fourth Amendment search. (BIO 10). The government asks this Court to categorically exclude all information in the hands of a third party from protection under the Fourth Amendment. For the reasons set forth in the Petition, it would be error for this Court to do so. (*See* Pet.

13-22). Furthermore, *Smith* and *Miller* do not dictate the outcome in the current digital age. (*Id*).

The government mechanically applies both the reasoning and the analysis in *Smith* and *Miller* to technology that was not even contemplated when these cases were decided. (BIO 11-16). The government equates the physical act of pressing buttons on a land-line telephone or the bank collecting or creating documents to the digital era where companies collect an unprecedented amount of information. These precedents, according to the government, need no revision, no limitation, and apply to the digital age. (BIO 13).

Furthermore, the government contents that Petitioner lacks a subjective expectation of privacy because (1) third parties create records for their own purposes and he voluntarily turned over his IP Login History to a third party. (BIO 13-14). According to the government, by using email, that person is "revealing his affairs to the [email provider]" and voluntarily taking the risk that the information that the email provider could record will be conveyed to the government. (BIO 14-15). The government demonstrates how expansively it reads *Smith* and *Miller* when it opined that "information that [Microsoft] had the facilities for recording and that it was free to record" remove any Fourth Amendment protections. (BIO 15). The government fails to appreciate the intrusiveness of the sensitive data collected by third parties as compared to previous technologies or analog data. The government is essentially stating that *Smith* and *Miller* provide limitless access to historical data without any judicial oversight. This Court should clarify the application of

Smith and *Miller* to digital records collected by third parties as people conduct their daily lives.

2. The government contends that law enforcement officers' ability to "infer" from Microsoft's records that petitioner used a computer at a particular location at a particular point in time is central to criminal investigations, and inferences do not amount to a search. (BIO 17). Inferences, however, do not insulate a search. *Kyllo v. United States*, 533 U.S. 27, 36-37 (2001). The government continually minimizes the locational data it is able to obtain from an IP Login History and instead states that the information it acquired in this case supported an inference that petitioner had accessed his email account at certain times from work and home but lacked many particulars. (BIO 20-21). The government requests this Court to apply *Smith* and *Miller* to current technology, so it may obtain invasive information without a warrant or court order under the third-party doctrine. (BIO 18-22).

The Seventh Circuit expressed concern at oral argument about the use of a person's IP Login History to track locational data.

> Court: And in the IP Login History, that allows the gov't to track a person's location as the person moves around the city, whether they log in from home or where—wherever, right?
>
> Government: I don't think it's that specific, your honor. My understanding of terms of—a lot has changed in the last few years in terms of mobile devices. My understanding is that a mobile device, such as a phone or an IPad or things like that, that they are generally assigned an IP address by their internet service provider, and that IP address will stay with them for at least some period of time, so if they are just going uptown or downtown in the course of a day, their IP address will stay the same. So, thus, just getting the IP Login history will not be able to necessarily track their movements as long as-- because it's still the same one IP address, there may be ways--

> Court- Where are they tracking it from?
>
> Government: I think, uh, what's happening is that the information is going to the internet service provider and they are sending it through to the mobile device—there may be—
>
> Court- By what means?
>
> Government: It may be something similar to the cell site information. So there may be—
>
> Court- Well, that's more specific then. Cell towers are—
>
> Government: That would be perhaps more precise location information, but that is not what is covered by the Stored Communication Act. Now in those cases, that is somewhat different. In those situations to get cell site information, generally my office would go to the courts to get [sic] order that information. That is something that is beyond what would be covered by the Stored Communications Act, beyond what would be permissible to get from an administrative subpoena. So that is where I think it becomes different. The IP Address does not necessarily give a [sic] precise information for a person. Now in this case, what happened here is that the defendant logged in using a home account which was tied to his home, so that case, the government was able to determine, or infer pretty reasonably that he was using his home to log in to Hotmail and he was using an account as his work to log into Hotmail…

(C.A. Oral Arg. at 17:55-20:08). The Seventh Circuit correctly questioned what type of information could be disclosed with an administrative subpoena. The government mistakenly argued that only the device's IP address would be visible, when actually, the IP address changes according to who is providing the internet service, including your coffee shop, your home router, the department store, and your doctor's office. The company who provides access to the internet assigns the IP address, and checking email reveals the IP address assigned at that location. The IP address collected by the web site or ISP is the final connection between the device and the

internet. The IP address combined with subscriber information allows the government to obtain information equally, if not more, invasive than GPS and with more specific location information than CSLI. (*See* Pet. 20-21). Contrary to the government's assertions, location need not be "inferred" when an IP address allows the government obtain specific location information, and any attempt to hide behind these alleged "inferences" is misplaced. (*See* BIO 22).

3. The government asserts that even if Petitioner has a privacy interest in Microsoft's records, "the government's acquisition of those records was reasonable and therefore complied with the Fourth Amendment." (BIO 23). As support, the government relies on "established law" that a person cannot invoke his Fourth Amendment rights to subpoenas of business records from a third party. (BIO 24 (citing *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 742 (1984)). *O'Brien*, however, involved an administrative investigation that adjudicated no legal rights. *Id.* The government's attempt to apply this same reasoning to a search involving a criminal investigations demonstrates its incredible overreach. The government is asking this Court to circumvent the requirements of the Fourth Amendment and find that its use of a subpoena to obtain records in the hands of a third party is constitutionally reasonable. (BIO 24). Under this theory, the amount of information that the government could obtain without oversight is limitless.

The government's argument that Petitioner could at most assert only a diminished expectation of privacy in the records held by Microsoft fails for the same reason. (BIO 25). As previously stated, the government wrongly asserts that

Petitioner's privacy interest was minimal, "given the limited nature of the location information that could be inferred from the IP-address records at issue here." IP Login History provides concrete locational information, and in Petitioner's case, no information needed to be inferred, because it provided Petitioner's exact location in his home. The government's argument has strong implications for current and future technology, and this Court stated, "While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36.

The government's suggestion that it has a compelling interest in issuing a subpoena rather than a warrant to seek information from third parties is misplaced at best. (BIO 25-26). The historical data here presented no timeliness issue or exigent circumstance, *see Riley v. California,* 134 S.Ct. 2473, 2485 (2014) ("There are no comparable risks [of harm to an officer or destruction of evidence] when the search is of digital data"), and the government would be hard pressed to cite evidence of such to support a new categorical approach to this type of data. "The claim that such a far-reaching intrusion on a reasonable expectation of privacy is reasonable without a warrant is a novel and dangerous approach to the Fourth Amendment, and should be rejected by this Court." *Carpenter v. United States,* No. 16-402, Reply Brief in Opposition, at *10 (filed 2/3/17).

III. This Case is an Excellent Vehicle to Decide this Issue, Because the Government Never Raised Any Argument that the Good-Faith Exception to the Exclusionary Rule Applied.

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 considering whether the government's unfettered requests for detailed, private information fall within the protections of the Fourth Amendment. Unlike other cases, there are no disputes of material fact and no procedural obstacles that would prohibit resolution of the merits of this case. The government's argument that the good-faith exception applies ignores the procedural history of this case. (BIO 29-30).

1. The government never raised any "good faith" argument in the district court. Motions to suppress evidence must be made before trial: "defenses, objections, and requests must be raised by pretrial motion if the basis for the motion is then reasonably available and the motion can be determined without a trial on the merits." Fed. R. Crim. P. 12(b)(3)(C); *see United States v. Daniels*, 803 F.3d 335, 351-52 (7th Cir. 2015). Rule 12 was amended in December 2014, during Petitioner's appeal, and although the revised rule deleted an earlier reference to "waiver," it did not alter the applicable standard that a court may consider a defense, objection, or request if the party shows good cause. Fed. R. Crim. P. 12(c)(3); *Daniels*, 803 F.3d at 352.

"Some circuit courts have read the newly amended version of Rule 12—in particular, the deletion of the reference to 'waiver'—to permit plain-error review

when a defendant did not intentionally relinquish a claim within Rule 12's ambit, even if the defendant has not offered good cause for his or her failure to timely raise it." *United States v. Burroughs*, 810 F.3d 833, 838 (D.C. Cir. 2016) (citing *United States v. Sperrazza*, 804 F.3d 1113, 1118-21 (11th Cir. 2015); *United States v. Soto*, 794 F.3d 635, 647-56 (6th Cir. 2015)). *Burroughs* noted that the Seventh and Eight Circuits "review unpreserved Rule 12 issues only when the defendant has made a showing of good cause, regardless of whether the defendant intentionally declined to raise those issues." *Burroughs*, 810 F.3d at 838 (citing *Daniels*, 803 F.3d at 351-52; *United States v. Anderson*, 783 F.3d 727, 741 (8th Cir. 2015). The D.C. Circuit in *Burroughs* did not decide which standard applied, because Burroughs made no showing of good cause. The same is true here.

2. The government's failure to raise any defense that the good-faith exception to the exclusionary rule would apply dooms its argument here. Both parties filed well-researched, thorough motions addressing Petitioner's arguments, and during the oral hearing, the government made no mention of any reliance on the good-faith exception. Furthermore, the government, without any legal citations or reasons for its failure to raise it below, mentioned good faith for the first time in its Appellee's Brief. (Gov't C.A. Br. 26-27; BIO 29). At oral argument, when asked about failing to raise the argument in the district court, the government responded, "It is true that the government did not argue good faith in the district court." (C.A. Oral Arg. at 22:17). In its decision, the Seventh Circuit made no mention of the government's good-faith defense. (App. A: 1-4).

Although the cases suggest that there is no consensus among the circuits on the review of unpreserved Rule 12 issues, the Court need not reach that issue in this case. As in *Burroughs*, the government has never argued or even attempted to make any showing that there was good cause for failing to raise the good-faith exception to the exclusionary rule. Therefore, the government's argument, that this case would be an unsuitable vehicle to address the question of the third party doctrine "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," wrongly overlooks its burden long ago to raise this issue or demonstrate good cause for failing to do so. (BIO 29-30). To now urge this Court to reject the petition on this basis is improper.

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