**No**.

October Term, 2021

IN THE
Supreme Court of the United States

ROBERT SOLOVE,
*Petitioner*,

v.

UNITED STATES OF AMERICA,
*Respondent*.

On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Eleventh Circuit

# PETITION FOR A WRIT OF CERTIORARI

MICHAEL CARUSO
FEDERAL PUBLIC DEFENDER
SCOTT BERRY
Assistant Federal Public Defender
Attorney for Petitioner
450 South Australian Ave, Suite 500
West Palm Beach, FL 33401
(561) 833-6288
Scott_Berry@fd.org

## QUESTION PRESENTED FOR REVIEW

In *Carpenter v. United States*, 138 S. Ct. 2206 (2018), this Court held that the government conducts a search under the Fourth Amendment when it accesses historical cell-site location records that provide a comprehensive chronicle of the user's past movements.

Here, the government accessed, without a warrant, historical records for a mobile application on Mr. Solove's cell phone. The records, which spanned a month, detailed all the internet protocol ("IP") addresses that the app had connected to during that time. Like the cell phone records in *Carpenter*, the historical IP addresses provided a comprehensive chronicle of Mr. Solove's movements during that month.

Question Presented:

**Whether the government conducts a search under the Fourth Amendment when it accesses historical IP address records for a mobile app that provide a comprehensive chronicle of the user's past movement?**

## INTERESTED PARTIES

There are no parties to the proceeding other than those named in the caption of the case.

## RELATED CASES

*United States v. Solove*, No. 20-CR-80025-DMM (S.D. Fla. 2021)

*United States v. Solove*, No. 21-11747, 2022 WL 152240 (11th Cir. Jan. 18, 2022).

## TABLE OF CONTENTS

QUESTION PRESENTED FOR REVIEW ..... i

INTERESTED PARTIES ..... ii

TABLE OF AUTHORITIES ..... iv

PETITION FOR WRIT OF CERTIORARI ..... 1

OPINION BELOW ..... 2

STATEMENT OF JURISDICTION ..... 2

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED ..... 2

STATUTORY AND OTHER PROVISIONS INVOLVED ..... 2

STATEMENT OF THE CASE ..... 3

STATEMENT OF FACTS ..... 4

REASONS FOR GRANTING THE WRIT ..... 6

CONCLUSION ..... 13

APPENDIX

Decision of the United States Court of Appeals for the Eleventh Circuit
*United States v. Solove*, No. 21-11747, 2022 WL 152240 (11th Cir. Jan. 18, 2022)
..... A-1

Judgment in a Criminal Case
*United States v. Solove,*
No. 18-cr-80025-DMM (S.D. Fla. May 20, 2021) ..... A-2

## TABLE OF AUTHORITIES

**CASES:**

*Carpenter v. United States*,

138 S. Ct. 2206 (2018) ..... i, 3, 6-8

*Riley v. California,*

573 U.S. 373 (2014) ..... 6

*Smith v. Maryland*,

442 U.S. 735 (1979) ..... 7-8

*United States v. Contreras,*

905 F.3d 853 (5th Cir. 2018) ..... 12

*United States v. Hood,*

920 F.3d 87 (1st Cir. 2019) ..... 12

*United States v. Miller*,

425 U.S. 435 (1976) ..... 7

*United States v. Morel,*

922 F.3d 1 (1st Cir. 2019) ..... 12

*United States v. Soybel,*

13 F.4th 585 (7th Cir. 2021) ..... 12

*United States v. Trader*,

981 F.3d 961 (11th Cir. 2020) ..... 3, 11-12

*United States v. VanDyck,*

776 F. App'x 495 (9th Cir. 2019) ..... 12

*United States v. Well-Beloved-Stone,*

777 F. App'x 605 (4th Cir. 2019) ..... 12

**CONSTITUTIONAL AND OTHER AUTHORITY:**

U.S. CONST., amend. IV ..... 2

18 U.S.C. § 2251(a) ..... 3

18 U.S.C. § 2251(e)(2) ..... 3

18 U.S.C. § 2252(a)(2) ..... 3

18 U.S.C. § 2252(a)(4)(B) ..... 3

18 U.S.C. § 2252(b)(1) ..... 3

18 U.S.C. § 2252(b)(2) ..... 3

18 U.S.C. § 3742 ..... 2

28 U.S.C. § 1254(1) ..... 2

28 U.S.C. § 1291 ..... 2

Sup. Ct. R. 13.1 ..... 2

Part III of the Rules of the Supreme Court of the United States ..... 2

A day in the life of your data, Australian Government: Be Connected, https://beconnected.esafety.gov.au/topic-library/essentials/all-about-data/home-data-vs-mobile-data/a-day-in-the-life-of-your-data ..... 9

Apple, If you can't receive email on your iPhone, iPad, or iPod touch, https://support.apple.com/en-ca/HT211082 ..... 10

Does A Smartphone Have An IP Address, (Jan. 6, 2021), https://smartphonedomain.com/does-a-smartphone-have-an-ip-address/ ..... 9

Google, Change Your Gmail Settings, https://support.google.com/mail/answer/6562?hl=en&co=GENIE.Platform%3DAndroid&oco=0 ..... 10

Kaspersky, What is an IP Address – Definition and Explanation, https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address ..... 8

Kristen Hicks, How IP Addresses Are Tracked, HostGator, (Feb. 13, 2020), https://www.hostgator.com/blog/how-ip-addresses-are-tracked/ ..... 8

Microsoft, How Can I Turn Push Notifications and Sounds On or Off?, https://support.microsoft.com/en-us/office/how-can-i-turn-push-notifications-and-sounds-on-or-off-ef8be4f4-85f9-4a90-8c4b-a27f483a0f0a ..... 10

Numbers, Facts and Trends Shaping Your World, Mobile Fact Sheet, PEW RESEARCH CENTER, (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ ..... 6

Website SEO Checker, IP Location – IP Look Up – Domain IP Look Up, https://websiteseochecker.com/ip-location/ ..... 9

**IN THE**
**SUPREME COURT OF THE UNITED STATES**

**OCTOBER TERM, 2017**

---

**No:**

**ROBERT SOLOVE,**

***Petitioner,***

**v.**

**UNITED STATES OF AMERICA,**

***Respondent.***

---

**On Petition for Writ of Certiorari to the**
**United States Court of Appeals**
**for the Eleventh Circuit**

---

# PETITION FOR WRIT OF CERTIORARI

---

Petitioner, Mr. Robert Solove, respectfully petitions the Supreme Court of the United States for a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit, rendered and entered in case number 21-11747, in that court on January 18, 2022, *United States v. Robert Solove,* no. 21-11747, 2022 WL 152240 (11th Cir. Jan. 18, 2022), which affirmed the judgment and commitment of the United States District Court for the Southern District of Florida

## OPINION BELOW

A copy of the decision of the United States Court of Appeals for the Eleventh Circuit, which affirmed the judgment and commitment of the United States District Court for the Southern District of Florida, is contained in the Appendix (A-1).

## STATEMENT OF JURISDICTION

Jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1) and Part III of the RULES OF THE SUPREME COURT OF THE UNITED STATES. The court of appeals entered its decision on January 18, 2022. Petitioner now timely files this petition pursuant to Sup. Ct. R. 13.1. The district court had jurisdiction because the government charged petitioner with violating federal criminal laws. The court of appeals had jurisdiction pursuant to 28 U.S.C. § 1291 and 18 U.S.C. § 3742, which provide that courts of appeals shall have jurisdiction for all final decisions and sentences of United States district courts.

## CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

Petitioner intends to rely upon the following constitutional provision:

**U.S. CONST., amend. IV**:

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

## STATEMENT OF THE CASE

### Course of Proceedings And Disposition In the District Court

Mr. Solove pled guilty to two counts of production, two counts of distribution, and one count of possession of child pornography in violation of 18 U.S.C. § 2251(a) and (e)(2), 18 U.S.C. § 2252(a)(2) and (b)(1), and 18 U.S.C. § 2252(a)(4)(B) and (b)(2), respectively. (DE 46). He reserved his right to appeal the district court's denial, without a hearing, of his motion to suppress evidence. (DE 15, 19, 46). The district court then sentenced him to a total of 600 months in prison, followed by supervised release for life and dismissed the remaining counts of the superseding information. (DE 68).

On appeal, relying on this Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), Mr. Solove argued that the government violated his Fourth Amendment rights when it obtained his IP address from a chat application called Kik without first procuring a warrant. Citing its own recent decision in *United States v. Trader*, 981 F.3d 961, 967 (2020), *reh'g en banc denied*, (Mar. 17, 2021), *cert denied*, 142 S. Ct. 296) No. 21-5323 (Oct. 4, 2021), the Eleventh Circuit affirmed Mr. Solove's conviction. *United States v. Solove*, 2022 WL 152240 (11th Cir. Jan. 18, 2022). Specifically, the Eleventh Circuit held that the third-party doctrine governed law enforcement's actions and that, as the Court had previously held in *Trader*, *Carpenter* constituted a very limited exception to that doctrine that did not apply to IP addresses. *Id.* at 1.

## Statement of Facts

On February 14, 2020, an undercover agent with the Department of Homeland Security ("HSI") contacted an unknown individual though an online chat application called Kik Messenger ("Kik"). (DE 50:19). The Kik user, under usernames rsolove99 and Rob_s, had posted a single image and two videos depicting child pornography in a group chat room. (DE 50:19). The undercover agent asked the user about the child depicted and the user replied that the girl was his daughter. (DE 50:19-20). The user sent a picture of himself and his daughter to the agent as proof the child was his own. (DE 50:20).

Rather than obtaining a warrant, law enforcement submitted an "emergency disclosure request" to Kik, requesting any IP addresses and user information for the individual associated with the *rsolove99* and *Rob_s* usernames. (DE 50:20). In response, Kik provided records for the 30-day period prior to the request, including among other things, the IP address used to post the child pornography. (DE 15:2; DE 50:20).

Law enforcement then used the IP addresses to learn the physical location of the device used to post the images, a particular residential address in Boca Raton, Florida. (DE 50:20). A records check revealed Mr. Solove registered his driver's license to that address, and the agents observed his driver's license photo resembled the person in the photograph the Kik user sent to the undercover agent. Based on this information, HSI obtained and then executed a search warrant for Mr. Solove's home. (DE 50:20).

During the search, HSI and the Palm Beach County Sheriff's Office seized various electronic devices, including two cellular phones. (DE 50:20-21). A later search of those cell phones yielded child pornography and evidence suggesting that Mr. Solove posted images and videos of child pornography depicting his own daughter in a chatroom. (DE 50:21-22). During and following the execution of the search warrant, law enforcement interrogated Mr. Solove and obtained statements from him regarding the same. (DE 50:22).

After the agents arrested Mr. Solove, they learned of a separate investigation wherein Mr. Solove had posted videos of a teenage female. (DE 50:22-23). In Mr. Solove's cell phones they recovered during the search, agents identified the female as a 14 year-old girl who resided in Oklahoma, and they confirmed that she and Mr. Solove exchanged videos of themselves masturbating. (DE 50:24). During their interview of her, she advised that Mr. Solove had requested, and she produced, the masturbatory videos. (DE 50:26).

Without first obtaining the IP addresses and user information from Kik, HSI could not have obtained the search warrant that ultimately led to the discovery of all of the evidence on Mr. Solove's phones or to his interrogation because they would not have been able to describe the particular area they wanted to search – his home. In short, until they obtained the IP addresses and user information from Kik, the agents did not know specifically who had posted the child pornography on the Kik application or the physical location of the devices used to post it.

## REASONS FOR GRANTING THE WRIT

**Like the seizure of cell-site location information in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the government's request and receipt of a month-long list of internet protocol addresses from the mobile application "Kik" provided access to a comprehensive chronicle of Mr. Solove's past movement and thereby constituted a warrantless search violating the Fourth Amendment.**

This case presents an important question of federal constitutional law which has not been, but should be, addressed by this Court: whether, under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the government conducts a Fourth Amendment search when it requests historical internet protocol ("IP") address records that provide a comprehensive chronicle of a smartphone user's past movements.

The vast majority of Americans – 85% of them – own a smartphone. *Numbers, Facts and Trends Shaping Your World, Mobile Fact Sheet*, PEW RESEARCH CENTER, (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/. And we "compulsively carry [them] all the time" through "public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales," so much so they have become "an important feature of the human anatomy." *Carpenter*, 138 S. Ct. at 2218 (citing *Riley v. California*, 573 U.S. 373, 385 (2014)). When the government tracks their location, "it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* The question presented herein thus asks whether the police may achieve such "near perfect surveillance," of virtually any American citizen, without a warrant.

### A. *Carpenter* recognized that cell phone data is worthy of Fourth Amendment protection.

In *Carpenter*, the Court held that the Fourth Amendment protects "a legitimate expectation of privacy in the record of [one's] physical movements as captured through cell-site location information ("CSLI"), and that law enforcement conducted an unlawful search when it obtained more than four months of CSLI from Carpenter's cell phone carrier without a warrant. *Id.* at 2217.

The Court found the "retrospective quality of the data" that CSLI provides gives "police access to a category of information otherwise unknowable" by allowing them to "travel back in time to retrace a person's whereabouts, subject only to the retention polices [sic] of the wireless carriers." *Id*. at 2218. The government "need not even know in advance whether they want to follow a particular individual, or when." *Id*. As a result, "[o]nly the few without cell phones could escape this tireless and absolute surveillance." *See id*.

Not only did this Court apply Fourth Amendment protection to CSLI, it also rejected an extension of the third-party doctrine. *Id*. at 2219-20; s*ee United States v. Miller*, 425 U.S. 435, 443 (1976); *Smith v. Maryland*, 442 U.S. 735, 742 (1979). In *Smith* and *Miller*, the Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Carpenter*, 138 S. Ct. at 2216 (citation omitted). "As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections." *Id*.

In *Carpenter*, the Court held that the third-party doctrine did not apply to CSLI because it "is not truly 'shared' as one normally understands the term." *Id.* at 2220. First, cell phones are such a "pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society." *Id.* (internal quotation marks and citation omitted). Second, a cell phone generates CSLI simply "by dint of operation." *Id.* Thus, "in no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements." *Id.* (*citing Smith*, 442 U.S. at 745) (internal quotation marks omitted). *Carpenter* thus establishes that the Fourth Amendment protects a privacy interest in third-party records of one's physical movements.

### B. IP addresses provide the same type of constitutionally protected data at issue in *Carpenter*.

Here, the government requested and received an analogous kind of information from which it could achieve the same retrospective surveillance that CSLI would have provided: IP address records. An IP address is a unique string of numbers and periods that identifies any device, including cell phones, connected to the internet. *What is an IP Address - Definition and Explanation*, KASPERSKY, https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address. ("Kaspersky"). It tells websites and applications where to send their data so the cell phone can access those parts of the internet. Kristen Hicks, *How IP Addresses Are Tracked*, HostGator, (Feb. 13, 2020), https://www.hostgator.com/blog/how-ip-addresses-are-tracked/. Each time a cell phone connects to the internet, the website

or application logs that device's IP address, including the date, time and duration of the connection. *Id*.

For mobile devices, like the smartphones in this case, the IP address changes each time that device connects to the internet through a different network because the device does not generate the IP address – the internet service provider or mobile network does. *Does A Smartphone Have An IP Address*, (Jan. 6, 2021), https://smartphonedomain.com/does-a-smartphone-have-an-ip-address/ ("Smartphone Domain"). As such, if the phone connects to the internet through a Wi-Fi network at a user's home, doctor's office, a coffee shop, or the airport, the network for each location will assign it a different IP address. Kaspersky. Moreover, if the phone connects to the internet using a mobile data plan rather than a Wi-Fi connection, the mobile service provider will assign yet another IP address. Smartphone Domain; *see also A day in the life of your data*, Australian Government: Be Connected, https://beconnected.esafety.gov.au/topic-library/essentials/all-about-data/home-data-vs-mobile-data/a-day-in-the-life-of-your-data (explaining how a cell phone switches from Wi-Fi to mobile data throughout the average user's day).

Once law enforcement determines the IP addresses a cell phone used to access an application like Kik, it can determine the device user's location when he or she accessed the application using a free, publicly available website. *See* Website SEO Checker, IP Location – IP Look Up – Domain IP Look Up, https://websiteseochecker.com/ip-location/. That site provides a location (country, city and latitude and longitude coordinates) detailing where the phone connected to the

internet, as well as the name of the internet service provider or mobile network the device used to access it. *Id*. Law enforcement can also contact the service provider to learn the network subscriber information, including the subscriber's physical address, as they did in this case. (DE 50:20). In short, law enforcement can map every location at which a user accessed that particular application. And because smartphones are constantly updating common applications by fetching data,[1] like email, they have the capacity to create IP address records even when the user is not intentionally accessing the application.

Thus, under *Carpenter*, the location data the government can learn from a month-long catalog of cell site data and the location data it can learn from a month-long catalog of IP addresses are the same. In each case, the data provides a comprehensive chronicle of an individual's movement, as if the government "had attached an ankle monitor to the phone's user." *Carpenter*, 138 S. Ct. at 2218.

**C. The decision below is wrong.**

Nonetheless, in Mr. Solove's case, the Eleventh Circuit declined to extend *Carpenter's* exception to the third-party doctrine to IP address records because "they

[1] Most common email applications default to frequently accessing email data in order to ensure users' inboxes are up-to-date. *See, e.g.*, Google, *Change Your Gmail Settings*, https://support.google.com/mail/answer/6562?hl=en&co=GENIE.Platform%3DAndroid&oco=0 (explaining that "Sync Gmail" setting "check[s] for emails automatically"); Microsoft, *How Can I Turn Push Notifications and Sounds On or Off?*, https://support.microsoft.com/en-us/office/how-can-i-turn-push-notifications-and-sounds-on-or-off-ef8be4f4-85f9-4a90-8c4b-a27f483a0f0a (cautioning that turning off notifications causes it "not . . . to fetch emails in the background); Apple, *If you can't receive email on your iPhone, iPad, or iPod touch*, https://support.apple.com/en-ca/HT211082 (describing "Mail Fetch" setting which determines "how your device receives email").

are neither location records nor cell phone records," "only reveal an individual's location indirectly," and "are associated with any device that can access a wireless internet network, including computers and tablets, rather than cell phones specifically." *Solove*, 2022 WL 152240 at 1. In so doing, the Eleventh Circuit cited its own prior precedent in *United States v. Trader*, 981 F.3d 961 (11th Cir. 2020)).

In *Trader*, the circuit court began with the faulty premise that "[a]bsent *Carpenter*, the third party doctrine would undoubtedly apply to the information the Government received from Kik." *Trader*. 981 F.3d at 967. Yet, even before *Carpenter*, this Court had not applied the third-party doctrine to data that provides a comprehensive chronicle of an individual's location over an extended period-of-time. Thus, even if this Court had not decided *Carpenter*, the Eleventh Circuit's opinion in *Trader* would have required an unsupported extension of the third-party doctrine.

As it stands, this Court did decide *Carpenter*, and the Eleventh Circuit has misapplied that decision as a mere limited exception to the third-party doctrine that applies "only to some cell-site location information, not to ordinary business records like email addresses and internet protocol addresses." *Trader,* 981 F.3d at 968. In so doing, the Eleventh Circuit ignored *Carpenter's* basic analytical framework: that the data's ability to provide a comprehensive chronicle of an individual's movement is what makes the third-party doctrine inapplicable. Moreover, the *Trader* Court incorrectly dismisses IP addresses as merely "a string of characters" that can only incidentally reveal location information, *id*. at 968-969, when, in reality, IP addresses, like cell site data, can easily provide an individual's location information

whenever that person's cell phone connects to the internet. *See* discussion *supra* pp. 13-15.

As the government did in *Carpenter*, law enforcement here conducted an unconstitutional search under the Fourth Amendment when it obtained a month-long data stream from Kik chronicling all of the IP addresses Mr. Solove's cell phone accessed through that application, without first obtaining a warrant. The district court erroneously denied Mr. Solove's motion to suppress. The Eleventh Circuit compounded the error by misapplying *Carpenter*.

### D. This case presents an important question of federal law warranting review.

The Eleventh Circuit is not alone in its misapplication of *Carpenter* to IP addresses. The First, Fourth, Fifth, Seventh and Ninth Circuits have issued similar rulings. *See United States v. Hood*, 920 F.3d 87 (1st Cir. 2019); *United States v. Morel*, 922 F.3d 1 (1st Cir. 2019); *United States v. Well-Beloved-Stone*, 777 F. App'x 605, 607 (4th Cir. 2019); *United States v. Contreras*, 905 F.3d 853 (5th Cir. 2018); *United States v. VanDyck*, 776 F. App'x 495, 496 (9th Cir. 2019); *United States v. Trader*, 981 F.3d 961 (11th Cir. 2020); *see also United States v. Soybel*, 13 F.4th 585 (7th Cir. 2021) (declining to extend Fourth Amendment protection to IP addresses collected with a pen register). Because these courts erroneously exempt IP addresses from the holding in *Carpenter*, they provide free license to governmental agents to track anyone with a cell phone – 85% of the population – by simply requesting historic IP address information that would provide them with essentially the same information they could get from cell site data. These circuits have created a significant loophole in the

Fourth Amendment privacy right this Court sought to protect in *Carpenter*. This case thus presents an important issue of federal law, warranting the Court's review.

## CONCLUSION

Based upon the foregoing petition, the Court should grant a writ of certiorari to the Court of Appeals for the Eleventh Circuit.

Respectfully submitted,

MICHAEL CARUSO
FEDERAL PUBLIC DEFENDER

By: *s/ Scott Berry*
Scott Berry
Assistant Federal Public Defender
Counsel For Petitioner Solove

West Palm Beach, Florida
April 15, 2022