

No. ____

October Term, 2020

IN THE
Supreme Court of the United States

SCOTT TRADER,
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
BERNARDO LOPEZ
Assistant Federal Public Defender
Attorney for Petitioner
1 E. Broward Blvd, Ste. 1100
Ft. Lauderdale, FL 33301
(954) 356-7436
Bernardo_Lopez@fd.org

AUGUST 6, 2021

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 phone records that provide a comprehensive chronicle of the user's past movements.

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

Question Presented:

Whether the Government conducts a search under the Fourth Amendment when it accesses historical I.P. 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. Trader, No. 17-cr-14047-DMM (S.D. Fla. 2017)

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
STATUTORY AND OTHER PROVISIONS INVOLVED	2
STATEMENT OF THE CASE.....	3
STATEMENT OF FACTS	4
REASONS FOR GRANTING THE WRIT	12
CONCLUSION.....	19
APPENDIX	
Decision of the Eleventh Circuit Court of Appeals, <i>United States v. Trader</i> , 981 F.3d 961 (11th Cir. 2020) No. 17-15611.....	
	A-1
Order Denying Petition for Rehearing En Banc <i>United States v. Trader</i> , (11th Cir. March 17, 2021) No. 17-15611.....	
	A-20
Petition for Rehearing En Banc <i>United States v. Trader</i> , (11th Cir. Feb. 10, 2021) No. 17-15611.....	
	A-21
Judgment in a Criminal Case <i>United States v. Trader</i> , No. 17-cr-14047-DMM (S.D. Fla. Dec. 8, 2017).....	
	A-47

TABLE OF AUTHORITIES

Cases:

Carpenter v. United States,

138 S. Ct. 2206 (2018) i, 4, 10-18

Smith v. Maryland,

442 U.S. 735 (1979) 14-16

United States v. Miller,

425 U.S. 435 (1976) 14-16

United States v. Trader,

981 F.3d 961 (11th Cir. 2020) 4, 10, 16

Constitutional and Other Authority:

U.S. Const., amend. IV i, 3, 4, 9, 10, 11, 13, 15, 17, 18

18 U.S.C. § 2251(a) 3, 9

18 U.S.C. § 2251(e)..... 3, 9

18 U.S.C. § 2252(a)(2) 3, 9

18 U.S.C. § 2252(a)(4)(B) 3, 9

18 U.S.C. § 2252(b)(1) 3, 9

18 U.S.C. § 2252(b)(2) 3, 9

18 U.S.C. § 2422(b) 3, 9

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
Lincoln Spector, Your Mobile IP Address: Its Safety Is One Thing, Its Privacy is Another, PC World, (Aug. 21, 2015), available at https://www.pcworld.com/article/2955112/your-mobile-ip-address-its- safety-is-one-thing-its-privacy-is-another.html	12
The Tech Wizard, What’s the Difference Between Wi-Fi and Data?, Available at https://thetechwizard.com/blog/wifi-cellular-data/	11
Website SEO Checker, IP Location – IP Look Up – Domain IP Look Up, available at https://websiteseochecker.com/ip-location/	12, 17

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

No:

**SCOTT TRADER,
*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. Scott Trader, 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 17-15611, in that court on November 25, 2020, *United States v. Trader*, 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 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 decision of the court of appeals was entered on November 25, 2020. Petitioner filed a timely petition for rehearing en banc. The petition for rehearing en banc was denied on March 17, 2021. This petition is timely filed pursuant to Sup. Ct. R. 13.1 and this Court's order of March 19, 2020. The district court had jurisdiction because petitioner was charged 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 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

On June 13, 2017, Mr. Trader was charged by indictment with: **Count 1**, enticing a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b); **Count 2**, distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); **Count 3**, possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2); and **Counts 4 and 5**, enticement of a minor to produce a sexually explicit video, in violation of 18 U.S.C. § 2251(a) and (e). (DE 7).

On September 6, 2017, Mr. Trader filed a motion to suppress illegally obtained evidence. (DE 13). The government responded. (DE 14). On September 25, 2017, the district court denied the motion and entered a written order. (DE 15).

Mr. Trader entered a conditional plea of guilty to Counts 1 – 5 on September 29, 2017, expressly reserving his right to appeal. (DE 18). The United States Probation Office concluded that Mr. Trader's Sentencing Guideline range was life imprisonment based upon an offense level of 43 and a criminal history category of III. Presentence Investigation Report (PSR). Mr. Trader filed a motion requesting a downward variance. (DE 34).

On December 7, 2017, the district court sentenced Mr. Trader to life imprisonment and a life time term of supervised release. (DE 37). Mr. Trader filed a timely notice of appeal on December 18, 2017. (DE 44).

On appeal, Mr. Trader argued that the government conducted a warrantless search in contravention of the Fourth Amendment when it accessed data from a

mobile app, Kik, that detailed all the Internet Protocol addresses connected to by Mr. Trader's cell phone through the Kik app for a period of a month. The Eleventh Circuit held that the government's action did not constitute a search under the Fourth Amendment. *United States v. Trader*, 981 F.3d 961 (11th Cir. 2020). Specifically, the Eleventh Circuit held that the actions of the government were governed by the third-party doctrine, and that this Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), constituted a very limited exception to the third-party doctrine that only applied to cell location data. Mr. Trader filed a petition for rehearing en banc arguing that the Eleventh Circuit's decision was directly contrary to this Court's decision in *Carpenter*. The Eleventh Circuit denied the petition for rehearing en banc.

Statement of Facts

On May 30, 2017, the police department of Thomasville, North Carolina received a complaint that several unknown men had engaged in inappropriate on-line sexual chats with the complainant's nine year old step-daughter, had sent the girl images of child pornography, and had requested that the girl send nude images of herself. (DE 1). The Thomasville police then contacted the U.S. Department of Homeland Security (HSI).

An HSI special agent in North Carolina inspected the girl's computer tablet and learned that the girl was accessing the social media service "Say Hi." "Say Hi" is a social media application for adults 18 and older. On her profile page, the girl claimed to be "Vitoria Jones," an adult, and had posted two "self-images" which

appeared to be a woman in her late twenties. (DE 1). The review further revealed that the suspect user went by the name “Scott.” (DE 1).

“Vitoria” began the “Say Hi” chat session with “Scott” by contacting him and asking: “Hi boyfriend. Can you chat please.” “Vitoria” then told “Scott” that she had a gift, “Jojo bows,” for his kids.¹ “Vitoria” then requested that “Scott” send pictures of his kids. “Scott” sent two pictures of fully clothed children and asks “Vitoria” to send a photo of her child. “Vitoria” sent a picture of a clothed adolescent female and made the comment: “My kids are cute,” followed by “I know honey our kids are cute.” To this point, “Vitoria” was clearly posing as an adult female with minor female children. Presentence Report (PSR), at 5.

“Scott” then asked “Vitoria” to send a picture of “your daughter naked.” “Vitoria” responded: “Yours frist.” (sic). “Scott” responded by sending what appears to be a widely circulated Internet nude image of an apparent adolescent female along with the statement: “My youngest daughter.” Approximately one minute later “Scott” sent a second nude female apparent adolescent image, also widely circulated on the Internet, and the comment: “My oldest daughter.” “Vitoria” then sent two nude images of an adolescent female to “Scott.” “Scott” then sent a short video of what appears to be an adult male rubbing his penis on the vagina of an adolescent female. He chatted that the video was “Me and my daughter.” (PSR at 5–8).

Approximately 20 minutes later, “Vitoria” again contacted “Scott” on “Say Hi” and sent “Scott” two nude images of herself. “Vitoria” requested nude photos of

¹ “Jojo Bows” are large colorful hair bows popular among adolescent females.

“Scott.” “Scott” sent a short video of a man masturbating and two still photos of an erect penis. “Vitoria” then requested a photo of “Scott’s” face. “Scott” sent a still photo of an adult male’s face. The image allegedly matched the facial image posted on “Scott’s” “Say Hi” user profile page. All communications between the girl and Scott took place over the “Say Hi” application. (PSR at 5–8).

HSI Special Agent Cory Brant who was investigating the complaint, noticed that “Scott’s” user profile on “Say Hi” indicated that he also was active on another social media service, “KiK,” under the user name “Daddyhasafunnyface.” Because “Say Hi” is a China-based company, Agent Brant was concerned that any request to “Say Hi” for “Scott’s” subscriber records would take too long. Consequently, he sent an “Emergency Situation Disclosure Request by Law Enforcement” to “KiK” instead. In that emergency request, Agent Brant claimed that the request involved a situation “involving death or serious physical injury.” Agent Brant then stated: “The KiK user identified below is believed to be actively molesting and sexually exploiting a minor in his custody and/or control. This subject is also involved in the sexual exploitation of other minors.” Agent Brant requested that “KiK” produce “the *last known customer name and email address and recent IP addresses* used by the account holder.” Agent Brant failed to inform “KiK” that its service was not used in the suspected illegal activity. (DE 1).

“KiK” responded with 29 pages, listing the “basic subscriber information, and the most recent 30 days of IP addresses if available associated with the Kik user name you provided.” The “subscriber information” included the email address associated

with the “KiK” account, “strader0227@yahoo.com.” It also showed that there were 594 logins to the “Daddyhasafunnyface” account from 42 different IP addresses during the 30 days prior to May 31, 2017. (DE 1).

Armed with the IP addresses and the email address, Agent Brant then sent an additional emergency disclosure demand to Comcast Corporation, the Internet provider for IP address “76.110.46.46.234 on 05/31/2017 at 6:36:32 UTC.” In that request, Agent Brant described the emergency as follows: “This subject is believed to have raped his daughter last night and sent videos depicting the rape to others. Since it appears that this subject is raping a child under his custody or control and the offenses are actively taking place this emergency request is being sought.” In the next section of the request, Agent Brant states: “The threat appears to be ongoing and the child is continually being sexually abused. It appears the child involved was sexually abused as early as last night.” Comcast responded that the subscriber to the IP address was assigned to “Shelly Trader, 1189 SW Edinburgh Dr., Port St. Lucie, 34953...” (DE 1).

Agent Brant then enlisted the assistance of HSI agents in the Southern District of Florida. HSI Special Agent Brian Ray conducted a property records search for the 1189 Edinburgh Drive residence and learned that it was purchased by Leon Bonano and Shelly Trader-Bonano on June 16, 2016. He also conducted a driver’s license records (DAVID) check of “Scott Trader.” Scott Trader’s residence address is listed in those records as 4286 Carl Street, Port St. Lucie, Florida. His mailing

address was listed as 1189 S.W. Edinburgh Drive, Port St. Lucie, Florida. (PSR at 8-9).

Agent Ray also ran a criminal records check on Scott Trader. It showed that Mr. Trader had been charged with Promoting a Sexual Performance by a Child, Lewd Behavior, and Possession of Child Pornography in 2012. All of those charges were dismissed and Mr. Trader pled no contest to a single count of Child Neglect. Mr. Trader was not “convicted;” adjudication was withheld. In December of 2016, Mr. Trader was charged with Lewd Behavior. He has pled not guilty and was on bond at the time of his arrest in this case. He is presumed innocent. (PSR at 9).

Finally, Agent Ray conducted a brief surveillance of 1189 S.W. Edinburgh Drive and witnessed an adult woman and a female child, approximately two years of age, enter the residence. He never saw Mr. Trader during the surveillance. (DE 1).

HSI agents then applied for a search warrant for 1189 Edinburgh Drive. HSI Special Agent Lori Cercy submitted a sworn affidavit in which she related the investigation of Agents Brant and Ray. On May 31, 2017, The Honorable William Matthewman, United States Magistrate Judge, signed a search warrant for the residence. (DE 1).

On June 1, 2017, the search warrant was executed. In a bedroom allegedly shared by Mr. Trader and his wife, agents located two smart phones, nine SD cards, and a portable hard drive. A forensic examination of these items revealed evidence of child pornography. Some of the photos/videos allegedly depicted Mr. Trader

involved in sexual behavior with minors. These items are the subject of the indictment in this case. (DE 1).

On June 13, 2017, Mr. Trader was charged by indictment with: **Count 1**, enticing a minor to engage in sexual activity, in violation of 18 U.S.C. § 2422(b); **Count 2**, distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1); **Count 3**, possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2); and **Counts 4 and 5**, enticement of a minor to produce a sexually explicit video, in violation of 18 U.S.C. § 2251(a) and (e). (DE 7).

On September 6, 2017, Mr. Trader filed a motion to suppress illegally obtained evidence. (DE 13). The government responded. (DE 14). On September 25, 2017, the district court denied the motion and entered a written order. (DE 15).

Mr. Trader entered a conditional plea of guilty to Counts 1 – 5 on September 29, 2017, expressly reserving his right to appeal. (DE 18). The United States Probation Office concluded that Mr. Trader's Sentencing Guideline range was life imprisonment, based upon an offense level of 43 and a criminal history category of III. Presentence Investigation Report (PSR). Mr. Trader filed a motion requesting a downward variance. (DE 34).

On December 7, 2017, the district court sentenced Mr. Trader to life imprisonment and a life time term of supervised release. (DE 37). Mr. Trader filed a timely notice of appeal on December 18, 2017. (DE 44).

On appeal, Mr. Trader argued that the government conducted a warrantless search in contravention of the Fourth Amendment when it accessed data from a

mobile app, Kik, that detailed all the Internet Protocol addresses connected to by Mr. Trader's cell phone through the Kik app for a period of a month. The Eleventh Circuit held that the government's action did not constitute a search under the Fourth Amendment. *United States v. Trader*, 981 F.3d 961 (11th Cir. 2020). Specifically, the Eleventh Circuit held that the actions of the government were governed by the third-party doctrine, and that this Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), constituted a very limited exception to the third-party doctrine that only applied to cell location data. Mr. Trader filed a petition for rehearing en banc arguing that the Eleventh Circuit's decision was directly contrary to this Court's decision in *Carpenter*. The Eleventh Circuit denied the petition for rehearing en banc.

REASONS FOR GRANTING THE WRIT

The holding of the Eleventh Circuit directly conflicts with this Court’s decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), where, like the cell tower information in *Carpenter*, the month-long list of internet protocol (“I.P.”) address provided by the mobile app “Kik” to police provided a comprehensive chronicle of Mr. Trader’s past movement during that month, and thus, the warrantless request for that information constituted a search under the Fourth Amendment.

Modern smartphones, which have become more akin to mini computers, allow users to gain access to two distinct information superhighways. The first information superhighway allows users to make telephone calls without being physically attached to another telephone via an array of wires. The second information superhighway, with wireless connections to the internet and with an endless number of smartphone applications (apps), allows smartphone users to send emails, connect to zoom meetings, start their cars, control lights and appliances in their homes, check the weather, accurately navigate any street in the world, book a flight, hail a ride, buy and sell stocks, communicate with individuals or with the entire world. *See* The Tech Wizard, What’s the Difference Between Wi-Fi and Data?, Available at <https://thetechwizard.com/blog/wifi-cellular-data/> (last visited Aug. 2, 2021). The possibilities are endless.

These two information superhighways each have their own distinct “on-ramps” for getting on that particular information superhighway. Telephone calls on wireless cellular phones require a network of cell towers that help transmit the telephone calls. A cell phone must connect to a cell tower to make or receive a telephone call. Companies keep detailed records of when a specific cell phone connects to a specific

cell tower, including the location of that specific tower, for purposes of making or receiving a telephone call. *Carpenter v. United States*, 138 S. Ct. 2206, 2211-12 (2018).

The second system involves the transmission of all other data that is not a telephone call. In this second system, a cell phone must connect to the internet through an Internet Portal (I.P.). Each I.P. has a distinct I.P. address. “Each device on the Internet has two I.P. addresses: a public one and a private one.” Lincoln Spector, Your Mobile IP Address: Its Safety Is One Thing, Its Privacy is Another, PC World, (Aug. 21, 2015), available at <https://www.pcworld.com/article/2955112/your-mobile-ip-address-its-safety-is-one-thing-its-privacy-is-another.html> (last visited Aug. 12, 2021). When you use your smartphone to connect to the internet, “[y]our private address connects you to the nearest cell tower. Your public address is one of many that connects your carrier’s network to the Internet.” *Id.* Companies keep detailed records of when a specific cell phone connects to a specific I.P. address, including the specific location of that I.P. address, for purposes of sending or receiving data. Thus, “[y]our carrier knows what IP addresses you were using at any given time. It also know where you have been.” *Id.* In fact, anyone can get a specific location of where a smartphone connected to the Internet with the public I.P. address. If an individual has the specific I.P. address, the individual can enter that specific I.P. address into a free tool on the Internet that will provide you with a precise location (Country, city and precise latitude and longitude coordinates) detailing where the smartphone connected to the internet. See Website SEO Checker, IP Location – IP

Look Up – Domain IP Look Up, available at <https://websiteseochecker.com/ip-location/> (last visited Aug. 2, 2021).

In *Carpenter*, this Court dealt with the data collected by companies associated with an individual's ability to make telephone calls from their cellular phones. As this Court noted, cellular phones connect with nearby cell towers. The telephone companies keep track of that information with date-stamped information that spells out when a specific telephone was nearby, and connect to, a specific cell tower. *Carpenter*, 138 S. Ct. at 2212. In *Carpenter*, this Court held that the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements. *Id.* at 2217.

Mr. Trader's case deals with the data collected by companies associated with an individual's ability to do everything else with a cellular phone, or more specifically, to connect to the internet from a cellular phone. Here, the government, without a warrant, got historic information from a company that runs a cellphone application called Kik regarding Mr. Trader's account with that company. Specifically, pursuant to the government's request, "Kik" responded with 29 pages, listing the "basic subscriber information, and the most recent 30 days of IP addresses if available associated with the Kik user name you provided." The "subscriber information" included the email address associated with the "KiK" account, "strader0227@yahoo.com." It also showed that there were 594 logins to the "Daddyhasafunnyface" account from 42 different IP addresses during the 30 days

prior to May 31, 2017. (DE 1). Because the IP addresses documented the precise time and location that Mr. Trader's cell phone accessed the internet through the Kik app, the data provided a comprehensive chronicle of Mr. Trader's movement for that 30-day period.

As this Court noted in *Carpenter*, government requests for digital data maintained by a third party that provides personal location information does not fit neatly under prior precedent but instead lies "at the intersection of two lines of cases." *Carpenter*, 138 S. Ct. at 2214. "The first set of cases addresses a person's expectation of privacy in physical location and movements." *Id.* at 2215. The second set of cases deals with the third-party doctrine where an individual has no legitimate expectation of privacy in information voluntarily turned over to third parties. *Id.* at 2216. Specifically, in *United States v. Miller*, 425 U.S. 435, 443 (1976), this Court held that an individual had no expectation of privacy in canceled checks, deposit slips and monthly statements kept by a financial institution. Subsequently, in *Smith v. Maryland*, 442 U.S. 735, 742 (1979), this Court extended *Miller* to information kept by the phone company noting the phone number called by an individual. In *Carpenter*, this Court expressly declined to extend *Smith* and *Miller* to the cell tower information accessed by the police.

This Court declined to extend *Smith* and *Miller*, even though the information was voluntarily turned over to a third party, because of the greater over-riding concern that the information allowed the police to chronicle an individual's movement for a long period of time:

We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection . . . we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.

Carpenter, 138 S. Ct. at 2217. This Court noted that the information was voluntarily given to a third party and that the records were generated for legitimate commercial purposes. Yet, this Court held that those distinctions did “not negate Carpenter’s anticipation of privacy in his physical location.” *Id.* In fact, this Court noted the heightened invasion on that privacy expectation where tracking the location of an individual’s cell phone allows the government to achieve “near perfect surveillance.” *Id.* at 2218. Even more troubling, this Court noted that “the retrospective quality of the data here gives police access to a category of information otherwise unknowable,” where essentially everyone with a cell phone has already been tracked. *Id.* Based on those over-riding concerns, this Court held that the Government’s access of that data “invaded Carpenter’s reasonable expectation of privacy in the whole of his physical movements.” *Id.* at 2219.

This Court also took pains to explain why the third-party doctrine simply did not apply to such pervasive location data. This Court stressed that *Smith* and *Miller* did not focus solely on the act of sharing, but rather “they considered the nature of the particular document sought to determine whether there is a legitimate expectation of privacy concerning their contents.” *Id.* at 2219 (internal citations and quotations omitted). In contrast, data that provides a “detailed chronicle of a person’s physical presence compiled every day, every moment, over several years . . .

implicates privacy concerns far beyond those considered in *Smith* and *Miller*.” *Id.* at 2220. This Court also noted that just about any activity on a cell phone including “checking for news, weather, or social media updates,” provides information that cannot really be considered to have been voluntarily provided. *Id.*

In its opinion, the Eleventh Circuit begins its erroneous holding with the faulty premise that “[a]bsent *Carpenter*, the third-party doctrine would undoubtedly apply to the information the Government received from Kik.” *United States v. Trader*, 981 F.3d 961, 967 (2020). That is a complete misreading not only of *Carpenter* but of *Smith* and *Miller* as well. In fact, even assuming *Carpenter* did not exist, applying the third-party doctrine to the information assessed by the Government would require an expansion of *Smith* and *Miller* and would ignore Mr. Trader’s expectation of privacy in the comprehensive location information accessed by the government. As this Court made clear in *Carpenter*, this Court has not applied the third-party doctrine to data that provide a comprehensive chronicle of an individual’s location over an extended period of time. So, even if this Court had not decided *Carpenter*, the Eleventh Circuit’s opinion here would have required an unsupported extension of *Smith* and *Miller*.

As it stands, this Court did decide *Carpenter*, and the Eleventh Circuit opinion here is a complete misapplication of this Court’s opinion in *Carpenter*. The Eleventh Circuit incorrectly treated *Carpenter* as a mere limited exception to the third-party doctrine. *Trader*, 981 F.3d at 967-968. And the Eleventh Circuit viewed that narrow exception as applying “only to some cell-site location information, not to ordinary

business records like email addresses and internet protocol addresses.” *Id.* at 968. In doing so, the Eleventh Circuit completely ignored this Court’s basic analytical framework in which this Court stressed that the ability to provide a comprehensive chronicle of an individual’s movement is the key characteristic of the data in question that makes the third-party doctrine inapplicable. The Eleventh Circuit inexplicably relies on cases from other circuits dealing with I.P. addresses even though it had to acknowledge that those cases were all decided prior to *Carpenter*. *Id.* at 968. Finally, the Eleventh Circuit incorrectly dismisses I.P. addresses as merely “a string of characters” that can only incidentally reveal location information. *Id.* at 968-969. The reality, of course, is that I.P. addresses, like cell site data, can provide a pinpoint location for an individual’s location via their cell phones whenever that cell phone connects or tries to connect to the internet. . See Website SEO Checker, IP Location – IP Look Up – Domain IP Look Up, available at <https://websiteseochecker.com/ip-location/> (last visited Aug. 2, 2021).

There is no difference under *Carpenter* for the location pinpoint data that can be gleamed from a month-long catalog of I.P. addresses collected from an individual’s cell phone and a month-long catalog of cell site data. In each case the data provide a comprehensive chronicle of an individual’s movement. And as with cell site data, the fact that the information accessed is historical means that the individual movement of anyone with a cell phone has already been chronicled. As in *Carpenter*, the police here conducted a warrantless search under the Fourth Amendment when they sought and received a month-long data stream from Kik chronicling all of the I.P. addresses

accessed by Mr. Trader's cell phone through the Kik app. The district court here, without the benefit of *Carpenter* which had not yet been decided, denied Mr. Trader's motion to suppress. The Eleventh Circuit compounded that error by misapplying *Carpenter*. That error has the potential to affect a large number of criminal defendants within the Eleventh Circuit and would allow the government to historically track anyone with a cell phone. Because the Eleventh Circuit's opinion takes I.P. addresses out of the holding in *Carpenter*, the government can easily track anyone with a cell phone by simply requesting historic I.P. address information that would provide them with essentially the same information they could get from cell site data. The government can thus circumvent the Fourth Amendment requirement of *Carpenter* and still freely track any individual with a cell phone. This Court must therefore grant Mr. Trader's petition and vacate the judgment of the Eleventh Circuit.

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

Fort Lauderdale, Florida
August 6, 2021

By: s/ Bernardo Lopez
Bernardo Lopez
Assistant Federal Public Defender
Counsel For Petitioner Trader