No. _____

In The
Supreme Court of the United States

KENDALL R. CARTER,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition For A Writ Of Certiorari To The United States Court Of Appeals For The Sixth Circuit

PETITION FOR A WRIT OF CERTIORARI

PETER J. STRIANSE*
TUNE, ENTREKIN & WHITE, P.C.
315 Deaderick Street, Suite 1700
Nashville, TN 37238
(615) 244-2770
pstrianse@tewlawfirm.com

Counsel for Petitioner
**Counsel of Record*

March 16, 2020

COCKLE LEGAL BRIEFS (800) 225-6964
WWW.COCKLELEGALBRIEFS.COM

QUESTIONS PRESENTED

Whether the Fourth Amendment warrant requirement guarantee protects a right to privacy in an internet protocol ("IP") address[1] and internet subscriber information to require federal agents investigating the electronic transmission of child pornography when agents acquired this information which revealed Carter's identity and address through federal administrative subpoenas[2] issued to a multi-media messaging service as well as a Tennessee-based internet service provider. In light of *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and the unique privacy interests at stake in this case, does the Fourth Amendment protect such IP address and internet subscriber information without application of the third-party doctrine?

---

[1] *IP address*: Residential internet customers typically connect to the internet through an internet service provider ("ISP"). Each time a customer connects, the ISP assigns a unique identifier, known as an IP address, to the customer's computer terminal. Depending on the ISP, a customer's IP address can change. IP addresses are conveyed to web sites that an internet user visits, and administrators of web sites can see the IP addresses of visitors to their sites. However, site administrators do not possess information linking a given IP address to a particular person. That information is held by the ISPs. *See United States v. Christie*, 624 F.3d 558, 563 (3d Cir. 2010).

[2] *Administrative subpoena*: (Sometimes known as a "desk subpoena.") This is a written request for information by law enforcement officers that does not require the actions of a grand jury or a judge. If law enforcement officers have probable cause, they can also obtain information using a grand jury subpoena, a search warrant issued by a judge, or a court order.

PARTIES TO THE PROCEEDING AND RULE 29.6 STATEMENT

Petitioner is Kendall R. Carter, defendant-appellant below. Respondent is the United States of America, plaintiff-appellee below. Petitioner is not a corporation.

STATEMENT OF RELATED CASES

- *United States v. Kendall R. Carter*, No. 3:15-cr-00162, U.S. District Court for the Middle District of Tennessee. Judgment entered Dec. 12, 2018.
- *United States v. Kendall R. Carter*, No. 18-6333, U.S. Court of Appeals for the Sixth Circuit. Judgment entered Oct. 16, 2019.

TABLE OF CONTENTS

TABLE OF CONTENTS – Continued

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES – Continued

PETITION FOR A WRIT OF CERTIORARI

Petitioner Kendall R. Carter respectfully petitions for a writ of certiorari to review the judgment and opinion of the United States Court of Appeals for the Sixth Circuit.

OPINIONS AND ORDERS BELOW

The opinion of the United States Court of Appeals for the Sixth Circuit affirming the judgment of the United States District Court for the Middle District of Tennessee is reproduced in the Appendix to this Petition at Pet. App. 1. That court's order denying rehearing is produced at Pet. App. 23. The judgment of the United States District Court for the Middle District of Tennessee is unpublished and is reproduced at Pet. App. 8.

JURISDICTION

The United States Court of Appeals for the Sixth Circuit entered judgment on October 16, 2019. Pet. App. 1. Mr. Carter filed a petition for panel rehearing and for rehearing *en banc*. That Court entered an Order denying the timely petition on November 21, 2019. Pet. App. 23. On January 13, 2020, this Court granted an application (No. 19A796) to extend the time to file a petition for a writ of certiorari until March 16, 2020.

This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

CONSTITUTIONAL PROVISIONS AND PROCEDURAL RULES INVOLVED

The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their person [and] houses . . . against unreasonable searches and seizures shall not be violated. . . ." U.S. Const. amend. IV. "Searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment – subject only to a few specifically established and well-delineated exceptions." *Katz v. United States*, 389 U.S. 347, 357 (1967).

INTRODUCTION

The Fourth Amendment to the United States Constitution provides that "[t]he right of the people to be secure in their person [and] houses . . . against unreasonable searches and seizures shall not be violated. . . ." U.S. Const. amend. IV. This clause guarantees a defendant's right to be free from unreasonable searches conducted outside the judicial process. Because a search occurs when a reasonable expectation of privacy is violated, law enforcement officers usually must obtain a warrant supported by probable cause. Here, there is a cognizable Fourth Amendment privacy interest in

an individual's subscriber information and IP address. Respectfully, the dated "third party doctrine" pronounced by this Court in the 1970s in *United States v. Miller*, 425 U.S. 435, 443 (1976) (government's warrantless acquisition of customer's bank records held by bank did not violate Fourth Amendment); and, *Smith v. Maryland*, 442 U.S. 735, 744-45 (1979) (warrantless collection of subscriber's phone calls did not violate Fourth Amendment), has been trumped by this Court's decision in *Carpenter v. United States*, 138 S.Ct. 2206 (2018). Therefore, consistent with *Carpenter*, IP address and internet subscriber information are protected under the Fourth Amendment and law enforcement officers who acquired such information through federally-authorized subpoenas were required to secure a court-issued search warrant to acquire the IP address and ISP information.

The *Carpenter* decision is in direct conflict with the "third party doctrine" precedent of this Court. Without clarification from this Court, this issue will recur. The Court should grant this petition to resolve this important and evolving issue.

STATEMENT OF THE CASE

1. Petitioner Kendall R. Carter was charged in the Middle District of Tennessee in a superseding indictment which charged twelve counts of production/attempted production of child pornography in violation of 18 U.S.C. §§ 2251(a) & (e), two counts of interstate

extortion in violation of 18 U.S.C. § 875(d), and one count of possessing child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) & 2252A(b) on November 18, 2015. On December 4, 2017, Mr. Carter entered a conditional plea of guilty to Counts 4, 6, 10, 14 and 15 of the superseding indictment, pursuant to Rule 11(a)(2), Fed.R.Crim.P., preserving his right to appeal, with the government's consent, the denial of his various suppression motions and the *Franks* hearing. On December 7, 2018, the district court sentenced Mr. Carter to a total term of imprisonment of 360 months followed by supervised release for life. Pet. App. 8. Defendant Carter remains incarcerated. Kendall Carter was 20 years old at the time of the alleged conduct. He was an outstanding college engineering student with no criminal history.

2. A Rutherford County, Tennessee, Sheriff's Department Detective was contacted in early November 2014 by a Special Agent of the North Dakota Bureau of Criminal Investigation regarding a sexual exploitation of a minor investigation with alleged ties to Rutherford County, Tennessee. The information developed to that point by State and federal authorities in North Dakota was that someone residing in Milton, Tennessee was communicating with an underage female in North Dakota utilizing a messaging application known as Kik Messenger. The alleged victim in North Dakota turned over her Apple iPod to law enforcement and it was forensically imaged. The North Dakota State Agent forwarded to the Tennessee Detective the results of certain forensic imaging from the

iPod, reports of investigation, and the results of administrative subpoenas directed to Kik Interactive, Inc., as well as to a Tennessee based internet services provider located in Alexandria, Tennessee. Armed with that information, the Tennessee Detective assembled and obtained a State search warrant from a Rutherford County Criminal Court Judge. In pertinent part, the Affidavit in support of the Tennessee search warrant summarized the investigation to date by explaining that the contents of a certain Apple iPod Touch used by a juvenile female in North Dakota were extracted by investigators; a certain Kik Messenger chat log occurring on September 14, 2014 at 3:46 a.m. Central Time was located; during the 9/14/14 chat the suspect instructed the juvenile female (MK) to take nude photos and videos and send them to certain screen names; a Department of Homeland Security Agent located in Grand Forks, North Dakota, obtained internet protocol (IP) records through "legal process from Kik Messenger" and determined that the usernames utilized an IP address located in Milton, Tennessee, and an iPhone and iPad were used to connect to Kik; and, the results of the Kik summons, received on November 3, 2014, indicated the subscriber associated with the IP address at the time and date of the Kik Messenger use, the 9/14/14 at 3:46 a.m. chat referred to earlier in the affidavit, was Kendall Carter located in Milton, Tennessee. With this information, the Tennessee Detective obtained and executed a search warrant for the address where Kendall Carter lived with his parents and three younger brothers. During the search, police seized a cell phone and an iPad which contained photos

and videos of child pornography. The federal charges followed.

REASONS FOR GRANTING THE PETITION

I. THE COURT'S *CARPENTER* DECISION IS IN DIRECT CONFLICT WITH THIS COURT'S "THIRD PARTY DOCTRINE" PRECEDENT.

Kendall Carter was entitled to suppression of the fruits of the illegal search of his home because the warrant in support of this search was based on information gathered in violation of his rights in light of *Carpenter*, 138 S. Ct. 2206 (2018). *Carpenter* evidences the continued acknowledgment and evolution of the right to privacy in digital information in the modern age, specifically when same relates to physical location or activities. *Carpenter*, 138 S. Ct. at 2214. *Carpenter* makes clear that the Fourth Amendment protects people not things. *Id*. Balancing the protection of the right to privacy provided to the individual with the increasing ability to gather information relating to the individual without a direct physical search of the person based on the changing technology and the increasing dependence of individual on digital devices in the modern world is a current concern of the Courts. *Id.* at 2213-16. *See also Kyllo v. United States*, 533 U.S. 27, 34 (2001) (Use of thermal imaging device to determine activity within a home absent physical search was still a search for purposes of the Fourth Amendment); *Riley v. California*, 573 U.S. 373, 393 (2014) (Holding a search of cell phone incident to arrest to be violative of

the Fourth Amendment given the storage capacity of modern phones, the degree of personal information they hold, and the ubiquitousness of these devices in modern society). *Kyllo*, *Riley*, and *Carpenter* all stand for the proposition that the protections offered under the Fourth Amendment must be viewed in light of the modern world and contextually applied so that the advance of technology is not a limitless intrusion into the privacy of the individual, any other approach leaves the individual "at the mercy of advancing technology." *Carpenter*, 138 S. Ct. at 2214 (citing *Kyllo*, 533 U.S. at 35).

Carpenter specifically addressed the concerns presented by the warrantless collection of historical cell site location information (CSLI) by law enforcement actors under the Stored Communications Act under 18 U.S.C. § 2701 *et seq*. *Carpenter*, 138 S. Ct. at 2221. CSLI is the records maintained by the wireless service provider which tracks which phones were connected to specific towers at historical times. *Id*., at 2211-12. The primary contention offered to support the warrantless seizure of these records under the SCA was the application of the third-party doctrine, i.e., that this information was shared with these third-party cell phone service providers and therefore no expectation of privacy by the individual exists, to assert that no warrant was required. Justice Alito in his dissent also advanced the argument that the use of compulsive but noninvasive administrative process such as the administrative subpoena procedure under the SCA should not be viewed in the same light as a traditional search since

the element of personal compulsion was not present. *Id*.

However, the majority rejected this line of reasoning and placed significance on the concern that the digital information in question here provided a historical record which indicated the location of the individual at different points in time and thus was the functional equivalent of physical surveillance. *Id*., at 2217. The *Carpenter* Court did acknowledge that certain exceptions, such as exigency would still apply to the warrant requirement adopted for CSLI. *Id*., at 2222. The Court also noted that the holding in *Carpenter* was narrow, addressing the matter then presented to the Court, yet they remained firm in the assertion that the "Court is obligated – as [s]ubtler and more far-reaching means of invading privacy have become available to the Government – to ensure that the 'progress of science' does not erode Fourth Amendment protections." *Id*., at 2223 (quoting *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) (Brandeis, J., dissent)).

The concerns of *Carpenter* are clearly reflected here in the collection of Kendall Carter's personal digital information which reflects his personal location spanning months through the collection of IP address information from his private digital communications. Significantly, Kik actually went beyond the limited information allowed to be produced in response to an administrative subpoena under the SCA. "The SCA provides privacy protection to communications held" in electronic storage by "providers of electronic communication service . . . and providers of remote computing

service." Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004), p. 1213-14. SCA Section 2703, which governs compelled disclosure of electronic communications, provides:

> Contents of wire or electronic communications in electronic storage. – A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

Importantly, the SCA draws a distinction between content, "the communication that a person wishes to share or communicate with another person," and non-content, "information about the communication that the network uses to deliver and process the content information" such as basic subscriber information. Kerr, *supra*, 1227-28. Kerr explains that "[t]he rules for compelled disclosure operate like an upside-down pyramid"

such that "[t]he higher up the pyramid you go, the more information the government can obtain." *Id*. at 1222.

> At the lowest threshold, only a simple subpoena is needed to compel basic subscriber information. Higher up the pyramid, a 2703(d) order compels all noncontent records. A simple subpoena combined with prior notice compels three categories of information: basic subscriber information, plus any opened e-mails or other permanently held files (covered by the RCS rules), plus any contents in temporary "electronic storage" such as retrieved e-mails in storage for more than 180 days. A 2703(d) order plus prior notice is sufficient to compel all noncontent records, plus any opened e-mails or other permanently held files (covered by the RCS rules), plus any contents in temporary "electronic storage" such as unretrieved e-mails in storage for more than 180 days. Put another way, a 2703(d) order plus prior notice compels everything except contents in temporary "electronic storage 180 days or less." Finally, a search warrant is needed to compel everything stored in an account. Id. at 1222-23 (footnotes omitted).

Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1195, 1208 (2010). Even before *Carpenter*, the information provided by Kik to federal law enforcement in North Dakota required a court order. In light of *Carpenter*, it required a search warrant.

The Sixth Circuit declined to apply the admonition of *Carpenter* to protect reasonable expectation of digital privacy of the individual even when portions of this information are necessarily shared with third parties through the operation of modern technology. Pet. App. ___. The Sixth Circuit never addressed the merits of Kendall Carter's *Carpenter* argument and summarily brushed it aside by retreating to the good-faith exception which it has broadly applied to searches that complied with the Stored Communications Act and then-binding case law. *Id.* The district court drew a distinction not present in *Carpenter* between a cell phone and the apps and programs on such a device. Such a distinction is not supported by *Riley*, relied upon by *Carpenter*, which specifically discussed the vast amount of personal information held on cell phones, including banking and financial information. *Riley*, 573 U.S. at 393-95. Such information is not stored as part of any cell phone's basic function of making a voice call, but rather is stored based on the use of the cell phone as a miniature computer to handle a broad range of activities and information. *Id*. at 395-98.

Yet, it was this information that *Riley* specifically protected, though it is clear that this information is not inherent or necessary to the basic operation of the phone and thus represents a choice by the user to be present on the phone. The question of the whether a warrant was necessary in *Carpenter* turned on whether there was a reasonable expectation of privacy that the Court, and by extension society, was willing to

protect and the level of personal surveillance that was offered by the relevant information. *Carpenter*, 138 S. Ct. at 2214-16. Neither of these concerns is negated in the present setting by the fact that the information in question stemmed from the use of an application on a phone rather than the inherent function of the cell phone. Kendall Carter clearly had an expectation of privacy regarding his private communications through use of the Kik messaging application. It was the use of the cell phone to communicate which generated digital records reflecting time, place, and activity which were improperly and effortlessly compiled by law enforcement officers without a warrant. This is exactly the concern addressed in *Carpenter* and suppression was warranted in this matter.

II. THIS CASE IS THE IDEAL VEHICLE FOR RESOLVING THIS IMPORTANT ISSUE.

Petitioner's case presents the ideal vehicle for this Court to resolve the conflict between the *Carpenter* decision and the dated "third party doctrine" precedent of this Court articulated in *Miller* and *Smith v. Maryland*. Kendall Carter explicitly preserved this question for appeal. He raised it in the district court and in the United States Court of Appeals for the Sixth Circuit. Unfortunately, the Sixth Circuit declined to address the issue on the merits and, at least, attempt to deal with the obvious conflict that exists between the "third party doctrine" and this Court's ruling in *Carpenter*. The question of whether an IP address and internet subscriber information are protected under the Fourth

Amendment and subject to the warrant requirement is an evolving and recurring issue.

CONCLUSION

For the foregoing reasons, the Court should grant the petition for a writ of certiorari.

Respectfully submitted,

PETER J. STRIANSE*
TUNE, ENTREKIN & WHITE, P.C.
315 Deaderick Street, Suite 1700
Nashville, TN 37238
(615) 244-2770
pstrianse@tewlawfirm.com

Counsel for Petitioner
**Counsel of Record*

March 16, 2020