Docket No. 10-1011

In the

SUPREME COURT OF THE UNITED STATES

March Term, 2019

HECTOR ESCATON,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Writ of Certiorari

*to **Case No. 18-3939**, Argued September 11, 2021—Decided November 2, 2021,*

of the United States Court of Appeals for the Fourteenth Circuit

---

BRIEF FOR PETITIONER

Team R4
Attorneys for Petitioner

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES Pages

CONSTITUTIONAL PROVISION

OTHER AUTHORITIES

QUESTIONS PRESENTED

I. Level of Suspicion Required for Forensic Searches at the Border:

Whether the Fourth Amendment requires that the government officers must have reasonable suspicion before conducting forensic searches of electronic devices at an international border.

II. Cell-Site Location Information Requests Under *Carpenter*:

Whether the government's acquisitions pursuant to 18 U.S.C. § 2703(d) of three days of cell-site location information, one-hundred cumulative hours of cell-site location information over two weeks, and cell-site location information collected from cell tower dumps violate the Fourth Amendment of an individual in light of this Court's limitation on the use of cell-site location information in *Carpenter v. United States*, 585 U.S. __ (2018).

OPINIONS BELOW

The decision of the United States Court of Appeal, for the Fourteenth Circuit, (affirming the decision of the United States District Court for the District of West Texas), is reported in *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021). (R. at 14). Both the District Court and the Court of Appeal concluded that Petitioner's Fourth Amendment rights were not violated. (R. at 14).

Circuit Judge Weber wrote a separate conclusion to which he concurred, in part, and dissented in part. (R. at 14). Judge Weber concurred with the majority decision to affirm the District Court's finding that no reasonable suspicion is required to conduct a forensic search at the border. Judge Weber also concurs with the majority decision with respect to finding that CSLI records from a tower dump does not constitute a search under the Fourth Amendment.

Judge Weber dissents, however, with the majority decision affirming the District Court's findings regarding law enforcement's CSLI requests for Petitioner's Three-day Records and Weekday Records.

CONSTITUTIONAL PROVISIONS AND RULES

This case involves the Fourth Amendment of the United States Constitution, which states:

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

U.S. Const. amend. IV.

Additionally, this case concerns governmental acquisitions pursuant to 18 U.S.C. § 2703(d), which states:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire of electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

18 U.S.C.A. § 2703 (West 2019)

STANDARD OF REVIEW

The High Court, in *U.S. v. Arvizu*, 534 U.S. 266 (2002), held that: the "[s]tandard for…review of reasonable-suspicion determinations is *de novo*, rather than 'abuse of

discretion.'" The Court, in *U.S. v. Williams,* 521 F.3d 902, 906 (8th Cir. 2008), held that: "[w]hether an individual has a reasonable expectation of privacy under the Fourth Amendment is a question of law [which is to be] reviewed *de novo*." *See United States v. Kiser,* 948 F.2d 418, 423 (8th Cir. 1991). The standard of review, concerning conclusions of law and the application of the law to the facts, is *de novo. See Wright v. West*, 505 U.S. 277, 297-98 (1992*)*; *Patton v. Yount,* 467 U.S. 1025, 1038 (1984); *Cuyler v. Sullivan,* 466 U.S. 345, 342 (1980).

INTRODUCTION

Petitioner's matter, under review by this Court, stems from his conviction regarding Bank Fraud, 18 U.S.C. § 1344, Conspiracy to Commit Bank Fraud, 18 U.S.C. § 1349, and Aggravated Identity Theft, 18 U.S.C. § 1028A. (R. at 6). Prior to trial, Hector Escaton, ("Petitioner"), filed a motion to suppress the results of: [1] a forensic search of his electronic devices while at the international border; and [2] cell-site location information, ("CSLI"), data collected from his wireless carrier. (R. at 6). As a result of the District Court's denial of this motion, Petitioner was convicted of the afore-mentioned charges. The Court of Appeal, for the Fourteenth Circuit, affirmed the District Court's order. (R. at 14).

Petitioner respectfully requests that this Court reverse the denial regarding the motion to suppress the results of the forensic search. This request is being made on the grounds that reasonable suspicion was required prior to any forensic search of an electronic device. In making this argument, Petitioner asserts that the Court of Appeal, for the Fourteenth Circuit, neglected to acknowledge the criteria set forth in *Touset*, which acknowledged that reasonable suspicion was present when an electronic search was conducted at an international border. Petitioner further asserts, that this court look to previously ascertained intelligence available—to

determine if reasonable suspicion exists—prior to Government agents conducting an electronic forensic search.

Additionally, Petitioner respectfully requests that this Court reverse the denial regarding the motion to suppress the results of the cell-site location information data collected. This argument is being made upon the grounds that the government's acquisitions of: [1] three days of cell-site location information; [2] one-hundred cumulative hours of cell-site location information over two weeks; and [3] cell-site location information collected from cell tower dumps **does constitute a search, *thus* violating protections *guaranteed* by the Fourth Amendment.** In making this argument, Petitioner asserts that the Court of Appeal, for the Fourteenth Circuit, erroneously read *Carpenter* as holding that *only* requests of CSLI *in excess* of seven days, or 168 hours, can constitute a search—thus violating an individual's Fourth Amendment expectation of privacy. Petitioner urges this Court to render an Order effectively stating that—there is no limited period for which the government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny. In providing clarity, Petitioner requests that this Court declare: CSLI requests, absent any exception, **are searches**, which invoke Fourth Amendment protections.

STATEMENT OF THE CASE

Petitioner was convicted of: [1] Bank Fraud, 18 U.S.C. § 1344, [2] Conspiracy to Commit Bank Fraud, 18 U.S.C. § 1349, and [3] Aggravated Identity Theft, 18 U.S.C. § 1028A. (R. at 6). Petitioner was convicted by the United States District Court for the District of West Texas in case number 1:18-cv-012345.

These convictions stem from a border checkpoint stop, occurring on September 25, 2019. (R. at 2). Petitioner—a West Texas citizen and resident—was stopped, and his vehicle was

inspected. (R. at 2). During this inspection, Officer Ashley Stubbs, of the Customs and Border Protection, ("CBP"), searched all of Petitioner's electronic devises. (R. at 2-3). Without any reasonable suspicion, (R. at 6), Officer Stubbs detained Petitioner's laptop, hard drives, and USB devises—which she submitted to the Immigration and Customs Enforcement, ("ICE"), to have forensically searched. (R. at 3). The information obtained as a result of this search—conducted without reasonable suspicion—ultimately resulted in Petitioner's afore-mentioned convictions.

ICE's forensic search, which was conducted without reasonable suspicion and took several hours, resulted in findings of traces of malware and documents containing individuals' bank account numbers and pins. (R. at 3). In turn, CBP contacted the Federal Bureau of Investigations, ("FBI"), which was subsequently working on a bank fraud investigation concerning ATM's at the Mariposa Bank branches in the city of Sweetwater. (R. at 3). Upon information from the Mariposa Bank, Hale also learned that the bank fraud included ATM's at the Mariposa Bank branches for the city of Escalante. (R. at 3).

Special Agent Hale, ("Hale"), working for the FBI, examined connections between the results of the forensic search—obtained without reasonable suspicion—and the Mariposa Bank fraud investigation for Sweetwater and Escalante. Upon receiving information of the trace malware from CBP, Hale reported Petitioner's information to the FBI for potential bank fraud and identity claims. (R. at 5). The malware found in Petitioner's possession was similar, *but not identical*, to the malware used in the Mariposa Bank in Sweetwater fraud. (R. at 5).

Hale, and U.S. Attorney Hughes, then requested Petitioner's historical cell-site location information records, ("CSLI"). (R. at 5). This request was granted and directed Delos Wireless—Petitioner's wireless carrier—to disclose information for "cell site records corresponding to [Petitioner's]…number…during the period of October 11, 2018 through October 13, 2018[.]" (R.

at 5). The result of this search placed Petitioner in the area of one of the Sweetwater branches on October 12, 2018. (R. at 5). However, these records **did not** place Petitioner near the town of Escalante.

As a result of no hard evidence to support a conviction, Hale further relied upon additional information obtained through the border checkpoint search, which was conducted without reasonable suspicion. (R. at 5). Hale identified a sticky note placed upon Petitioner's laptop. This sticky note contained a name and number for "Delores". (R. at 5). Suspecting that this name and number *may* contain information regarding the bank fraud, Hale requested a second CSLI. (R. at 5). This second request consisted of CSLI information for both Delores and Petitioner's CSLI for "all weekday records between October 1 and 12 between the hours of 8 AM MDT and 6 PM MDT, as well as all subscriber information for 'Delores's; telephone…" (R. at 5). The requested period of CSLI covers ten weeks during typical business working hours, totaling 100 hours. Seven days of CSLI totals 168 hours. (R. at 5).

Upon the result of the CSLI, Hale learned that telephone information on the note belonged to Delores Abernathy—who had been previously convicted of ATM skimming—bank fraud. (R. at 5). Abernathy was indicted and a search warrant was provided for her home. (R. at 5). In her home, law enforcement found cash and malware. (R. at 5). Abernathy was subsequently arrested. (R. at 5). After she was arrested, Abernathy entered into a plea deal and cooperated with the government in a case against Petitioner. (R. at 6).

ARGUMENT

I. THE FOURTH AMENDMENT *DOES* REQUIRE—AT AN INTERNATIONAL BORDER—THAT GOVERNMENT OFFICERS *MUST* HAVE REASONABLE SUSPICION *BEFORE* CONDUCTING FORENSIC SEARCHES OF ELECTRONIC DEVICES.

Pursuant to the Fourth Amendment of the United States Constitution an individuals right to "to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const., amend. IV. Courts have addressed issues pursuant to the Fourth Amendment and have attempted to define what constitutes "searches and seizures."

The Court in *United States v. Touset,* 890 F.3d 1227 (11th Cir. 2018), had determined that forensic searches that take place at the border, did not require reasonable suspicion. In fact, the court in *United States v. Ramsey,* 431 U.S. 606, 619 (1977) determined border searches "have been considered to be 'reasonable' by the single fact that the person or item in question had entered into our country from outside. There has never been any additional requirement that the reasonableness of a border search depended on the existence of probable cause." (R. at 7).

Despite these findings that searches at the border may occur without reasonable suspicion or an additional requirement of probable cause, the *Touset Court* makes it a point that "reasonable suspicion existed for the forensic searches of Touset's Electronic Devices." *Touset,* 890 F. 3d at 1237. The ''inquiry focuses on the information available to the officers at the time of the stop.'' *United States v. Lewis*, 674 F.3d 1298, 1305 (11th Cir. 2012).

A. THE COURT OF APPEAL FOR THE FOURTEENTH CIRCUIT NEGLECTS TO ACKNOWLEDGE THE COURT'S JUSTIFICATION IN *TOUSET*, AS IT SERVES AS A COMPASS WHEN DETERMINING IF REASONABLE SUSPICION IS NECESSARY TO CONDUCT A CELLUALR SEARCH AT THE BORDER

In *Touset* 890 F.3d at 1237 the government had a "particularized and objective basis for suspecting" *Touset* possessed child pornography on his electronic devices. Here, Customs and Border Protection Officer Stubbs had no prior knowledge of any activity, data, or hash values that would have provided Ms. Stubbs with reason to believe Mr. Escanton was involved in prior criminal activity. (R. at 3). The Border Patrol Agent's in *Touset*, had prior knowledge that Touset

sent three prior money transfers to a Western Union account that was associated with cellular and email accounts that contained pornography. *Touset* 890 F.3d at 1237. However, Government officials here obtained the "documents containing individual's bank account numbers and pins, and malware information," after the electronics were delivered to a Computer Forensic examiner. (R. at 3).

a. THE COURT IN *TOUSET*, ACKNOWLEDGED REASONABLE SUSPICION WAS PRESENT AS A RESULT OF PRIOR GOVERNMENT INVESTIGATIONS

A significant distinction exists when evaluating if reasonable suspicion is necessary to conduct a cellular device search at the border. The *Touset Court* concluded that "this evidence provided reasonable suspicion for the forensic searches of Touset' s electronic devices." *Touset,* 890 F. 3d at 1237. In addition to this concession, the government agreed "that the applicable fourth amendment test was whether there was reasonable suspicion of criminal activity such that border agents could detain Touset's electronic devices for forensic analysis." *Touset,* 890 F. 3d at 1238. "After a series of investigations by private organizations and the government suggested that Karl Touset was involved with child pornography, border agents forensically searched his electronic devices after he arrived at the Atlanta airport on an international flight." *Touset,* 890 F. 3d at 1230.

b. IN ORDER TO ASSURE MAXIMUM SECURITY AT THE BORDER, REASONBLE SUSPICION MUST BE REQUIRED BEFORE CONDUCTING A FORENSIC SEARCH OF AN ELECTRONIC DEVICE.

"The Government's interest in preventing the entry of unwanted persons and effects is at its zenith at the international border." *U.S. v. Flores-Montano* 541 U.S. 149, 153 (2004). The requirement of reasonable suspicion at the border, will assure that Government agents are equipped with the necessary intelligence and valuable knowledge to anticipate the arrival of any

unwanted person or entry. The *Flores-Montano Court* described the interest of protecting the border and stated "interest in protecting the borders is illustrated in this case by the evidence that smugglers frequently attempt to penetrate our borders with contraband secreted in their automobiles' fuel tank. Over the past 5 ½ fiscal years, there have been 18,788 vehicle drug seizures at the southern California ports of entry. App. to Pet. for Cert. 12a. Of those 18,788, gas tank drug seizures have accounted for 4,619 of the vehicle drug seizures, or approximately 25%." This data acquired over the prior 5 years is an authentic example of intelligence Border Patrol Agents having prior information available to them, thus allowing them to have reasonable suspicion when conducting vehicle searches at border entries. *Flores –Montano,* 541 U.S. at 1586.

c. A FORENSIC SEARCH OF AN ELECTRONIC DEVICE IS A UNIVERSAL ACT THAT IS CONDUCTED BY BOTH LAW ENFORCEMENT AND BORDER PATROL AGENTS

Here, the court neglected to follow the court's ruling in *Riley v. California,* 573 U.S. 2480 (2014) because "Riley addressed a different question: whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." (R. at 9). However, though the court believes that *Riley*, provides no clarification of border forensic searches, it fails to distinguish what makes a forensic search of an electronic device different at the border or after an arrest. It is not enough to justify the search of a cellular device because of the location where it is occurring.

d. REASONABLE SUSPICION ELIMINATES JUDICIAL SECOND GUESSING WHEN ATTEMPTING TO CONDUCT A CELLULAR DEVICE SEARCH AT AN INTERNATIONAL BORDER.

In *Touset*, the court held that the increasing sophistication of technology "only heightens the need of the government to search property at the border unencumbered by judicial second guessing." *Touset,* 890 F. 3d at 1235. Because reasonable suspicion would require agents to have

prior knowledge or intelligence about one's entry at the border, judicial second guessing would no longer be an issue. However, if reasonable suspicion is not implemented in regard to conducting a cellular device search at the border, there would be no protection from judicial issues and second guessing. In *Flores-Montano,* the court held, "the expectation of privacy is less at the border than it is in the interior." *Flores-Montano* 541 U.S. at 1583. This diminished expectation of privacy is a contributing factor to judicial second guessing. Diminished expectation of privacy should not result in the diminished expectation of a U.S. citizens constitutional right.

II. THE GOVERNMENT'S ACQUISITIONS OF: [1] THREE DAYS OF CELL-SITE LOCATION INFORMATION; [2] ONE-HUNDRED CUMULATIVE HOURS OF CELL-SITE LOCATION INFORMATION OVER TWO WEEKS; AND [3] CELL-SITE LOCATION INFORMATION COLLECTED FROM CELL TOWER DUMPS—PURSUANT TO 18 U.S.C. § 2703(d)—*DOES VIOLATE* THE FOURTH AMENDMENT OF AN INDIVIDUAL—IN LIGHT OF THIS COURT'S LIMITATION ON THE USE OF CELL-SITE LOCATION INFORMATION IN *CARPENTER V. UNITED STATES*, 585 U.S. __ (2018).

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const., amend. IV. The basic "purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by government officials." *Camera v. Municipal Court of City and County of San Francisco,* 387 U.S. 523, 528 (1967). In *Katz v. United States,* 389 U.S. 347, 351 (1967), the High Court established that "the Fourth Amendment protects people, not places," and expanded the conception of the Amendment to protect certain expectations of privacy, as well. Indeed, the Court stated that the Fourth Amendment protects not only property interests, but also reasonable expectations of privacy. *Id.* Thus, when an individual "seeks to preserve something as private," and the expectation of privacy is "one that society is prepared to recognize as reasonable," it is held that intrusion into

the private sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith v. Maryland,* 442 U.S. 735, 740 (1979).

For issues of law concerning the Fourth Amendment, the Court has historically focused on whether the Government "obtain[ed] information by physically intruding on a constitutionally protected area." *United States v. Jones,* 565 U.S. 400, 405, 406, n. 3 (2012). In determining whether search and seizures are unreasonable, the Court, in *Carpenter v. United States,* 585 U.S. __ (2018) (slip op.), relied upon two guideposts. First, the Court recognized that the Amendment "seeks to secure the privacies of life against arbitrary power." *Boyd v. United States,* 116 U.S. 616, 630 (1886). Second, the Court distinguished that the Amendment seeks "to place obstacles in the way of a too permeating police surveillance. *United States v. Di Re,* 332 U.S. 581, 595 (1948). As technology continues to advance, allowing the Government the capacity to encroach upon areas normally guarded from inquisitive eyes, the Court remarked that it has continuously sought to "assure[] preservation of that degree of privacy against government…" *Kyllo v. United States,* 533 U.S. 27, 34 (2001).

The *Carpenter Court* acknowledged that cell phones, and the services they provide, are "such a pervasive and insistent part of daily life" that "carrying one is indispensable to participation in modern society." *Carpenter,* 585 U.S. __ (slip op., at 3). In doing so, the Court distinguished that "historical cell-site records present even greater privacy concerns…[because] a cell phone [is] almost a 'feature of human anatomy,'…[and] tracks nearly every movement of its owner." *Id.* at p. 13. Indeed, the Court recognized that "CSLI is an entirely different species…[which] implicates basic Fourth Amendment concerns about arbitrary government power." *Id.* at p. 20. And, while the Court indicated case-specific exceptions—such as exigent circumstances—may apply to compel documents without probable cause, it should not be

understated that the dominant theme regarding access to CSLI is that the "Government will generally need a warrant." *Id.* at p. 25.

The Court concluded, in *Carpenter,* 585 U.S. __ (slip op.), that to ensure that the "progress of science" does not erode the Fourth Amendment protection, the Court was required to decline a *grant* to the state of unrestricted access to a wireless carrier's database of physical location information. *Id.* at p. 22. In its reasoning, the Court opined that: "[i]n light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment Protection." *Id.* at p. 22.

A. THE COURT OF APPEAL, FOR THE FOURTEENTH CIRCUIT, ERRONEOUSLY READS *CARPENTER* AS HOLDING THAT ONLY SEVEN DAYS OR MORE OF CSLI CAN VIOLATE AN INDIVIDUAL'S EXPECTATION OF PRIVACY

The Supreme Court, in *Carpenter*, did "not decide whether there [was] a limited period for which the government may obtain an individual's historical CSLI free from Fourth Amendment Scrutiny, and if so, how long that period may be." *Carpenter,* 585 U.S. __ (slip op., at 11, 11 n.3). The Court simply stated—in a footnote—that it was "sufficient for [its] purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search." *Id.* In making this assertion, the Court focused on the propriety of seven days simply because "the Government treat[ed] the seven days of CSLI requested from [the wireless carrier] as the pertinent period, even though [the wireless carrier] produced only two days of records. *Id.*

Undoubtedly, the Court decided *Carpenter* upon the facts presently before it. *Carpenter,* 585 U.S. __ (slip op.). Indeed, it is noted in the dissent of the Appeal, that: "the Court did not indicate—much less hold—that a *shorter* period of time would not violate an individual's expectation of privacy." (R. at 15; emphasis added). Moreover, the Court affirmatively stated

that the "government *must* generally obtain a warrant supported by probable cause *before* acquiring such records." *Carpenter,* 585 U.S. __ (slip op., at 18; emphasis added). It is without question that the Court of Appeals, for the Fourteenth Circuit, erroneously read *Carpenter* to hold that only seven days or more of CSLI can violate an individual's expectation of privacy.

a. A DECISION NEEDS TO BE MADE, BY THIS COURT, CLARIFYING THAT ALL CSLI REQUESTS—ABSENT ANY EXCEPTION—ARE SEARCHES, INVOKING FOURTH AMENDMENT PROTECTIONS, REGARDLESS OF THEIR TIMEFRAME.

Petitioner's case comes before this Court ripe for review. "For a suit to be 'ripe' within the meaning of Article III, it must present concrete legal issues, presented in actual cases, not abstractions. U.S. Const. art. 3, § 2, cl. 1. Petitioner's case *does* present concrete legal issues because the Court, in *Carpenter*, **did not** decide whether there was a limited period for which the government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny. *Carpenter,* 585 U.S. __ (slip op., at 11, 11 n.3); (R. at 15). As a result of not deciding whether there was a limited period for which the government may obtain an individual's historical CSLI, the Court of Appeal, for the Fourteenth Circuit, erroneously read *Carpenter* to hold that only historical CSLI requests *of more than* seven days, or 168 hours, constituted a search. This reading is erroneous because it understates the High Court's rationale that seven days, or 168 hours, was "sufficient for [the Court's] purposes…" (R. at 15) because that was the factual time span before the Court. Thus, the Court of Appeal found, in Petitioner's case, that there was no search involved, to invoke Fourth Amendment protections, when law enforcement requested CSLI information which seemingly circumvents the perceived time limitations of *Carpenter.* As a result, an actual injury *did* occur because Petitioner *was* convicted under the same nucleus of operative facts which reversed Carpenter's conviction—baring the time element.

Without a decision determining whether there is a limited period for which the government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, the Courts, and law enforcement, will deliberately continue to side-step of limitations placed in *Carpenter,* seemingly misunderstanding the true message in *Carpenter,* which stated: "get a warrant." *Carpenter,* 585 U.S. __ (slip op., at 19).

Therefore, this Court must provide clarification by holding that all CSLI requests—absent any exception—are searches, invoking fourth amendment protections, regardless of their timeframe.

b. *CARPENTER* EMPHATICALLY HOLDS THAT GOVERNMENT ACQUISITION OF CELL-SITE RECORDS IS A FOURTH AMENDMENT SEARCH—THUS, REQUIRING A WARRANT FOR REQUESTS FOR FEWER THAN SEVEN DAYS OF DATA.

The Court, in *Carpenter,* unambiguously denied law enforcement the allowance of unrestricted access to CSLI records by stating such actions *are* a search invoking Fourth Amendment protections. In simplistic, unwavering clarity, the Court stated in *Carpenter* that: "[w]e decline to grant the state unrestricted access to a wireless carrier's database of physical location information." *Carpenter,* 585 U.S. __ (slip op., at 22).

The Court, in *Carpenter*, "found that the acquisition of Carpenter's CSLI was a search." *Carpenter,* 585 U.S. __ (slip op., at 18). In concluding that the acquisition of Carpenter's CSLI records was a search, the Court observed that "the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id*. Perhaps most notably, as it pertains to both *Carpenter* and Petitioner's case, is the Court's assertion that: "a search is undertaken by law enforcement officials to discover evidence *of a wrongdoing*." *Veronica School Dist. 47J v. Acton,* 515 U.S. 646, 652-653 (1995); emphasis added. And a search, "[i]n

the absence of a warrant…is [only] reasonable if it falls within a specific exception to the warrant requirement." *Riley v. California,* 573 U.S. __ (2014) (slip op., at 5).

Without question, the Court found the acquisition of Carpenter's CSLI *did* constitute a—warrantless—search; thus, Carpenter's conviction was reversed. Moreover, the Court declined to *grant* the state unrestricted access to a wireless carrier's database of physical location information. Instead, the Court admonished, with regards to CSLI, that—absent any exception, such as exigent circumstances—the Government will generally need a warrant.

c. THE INTRINSIC FACTS OF PETITIONER'S CASE ARE IDENTICAL TO THE OPERATIVE FACTS IN *CARPENTER*—THUS, WARRANTING A REVERSAL OF PETITIONER'S CONVICTION ON THE GROUNDS THAT THE CSLI RECORDS—OBTAINED IN A SERACH WITHOUT PROBABLE CAUSE—DID VIOLATE PETITIONER'S FOURTH AMENDMENT RIGHTS

The Court, in *Carpenter*, found that "the government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show 'reasonable grounds' for believing that the records were 'relevant and material to an ongoing investigation.'" *Carpenter,* 585 U.S. __ (slip op., at 3); 18 U.S.C. § 2703(d). These operative facts—when juxtaposed against Petitioner's case—are indistinguishable because law enforcement obtained Petitioner's cell-site information pursuant to 18 U.S.C. § 2703(d), as well. (R. at 4).

i. FACTS AS THEY RELATE TO CARPENTER

In *Carpenter,* four men suspected of robbing a series of Radio Shacks and T-Mobile stores were arrested. One person confessed to the acts and identified 15 accomplices who participated in the heists. This person additionally gave law enforcement his call records to identify additional numbers. Based from this information, law enforcement obtained record

information regarding Carpenter—which further provided the necessary information needed for Carpenter's conviction.

Specifically, law enforcement obtained two orders under Carpenter's information. The first order—MetroPCS—was for disclosure of cell-site information during a four-month period. The order sought cell-site information for 152 days, but only received cell-site information for 127. The second order—Sprint—requested cell-site information for seven days, but only two days of cell-site information were produced. *Carpenter,* 585 U.S. __ (slip op., at 3). Prior to obtaining this CSLI information, law enforcement undeniably did not have enough information to support a conviction. Law enforcement used the information provided by Carpenter's co-defendant to review Carpenter's movements—retroactively—until they obtained enough evidence to support a conviction.

In finding that the ordered production of these records constituted a search in violation of the Fourth Amendment, the Court stated that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. *Carpenter,* 585 U.S. __ (slip op., at 11.) The Court further acknowledged that CSLI mapping "provides an all-encompassing record of the holder's whereabouts…provid[ing] an intimate window into a person's life…revealing not only…particular movements, but…many…'privacies of life.'" *Id.* at p. 12. The Court noted that "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences…achiev[ing] near perfect surveillance." *Id.* at p. 12-13; emphasis added). Perhaps most importantly, the Court acknowledged that: "cell phones and the services they provide are such a pervasive and insistent part of daily life" and "that carrying one is indispensable to participation in modern society." *Id.* at p. 3.

Consequently, the Court stated that "an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant." *Carpenter,* 585 U.S. __ (slip op., at 19).

ii. FACTS AS THEY RELATE TO PETITIONER

Petitioner's case is factual indistinguishable from *Carpenter,* but for law enforcement's deliberate attempt to side-step the perceived time constraints of *Carpenter.* Petitioner's case is factual similar to *Carpenter.* In both cases, there was another person who was arrested in connection to the alleged crime. (R. at 5). Like Carpenter, a co-defendant in Petitioner's case was arrested, confessed, and assisted law enforcement in charges against Petitioner by providing cell phone numbers and information. (R. at 5).

In Petitioner's case, law enforcement—seemingly having knowledge of the ruling in *Carpenter* because their CSLI request comported to the time constraints perceived in *Carpenter*—specifically sought: [1] three days of cell-site location information; [2] one-hundred cumulative hours of cell-site location information over two weeks; and [3] cell-site location information collected from cell tower dumps. (R. at 5). Like Carpenter, law enforcement did not have enough information necessary for a full conviction. (R. at 5). Law enforcement used the information provided by Petitioner's co-defendant to review Petitioner's movements—retroactively—until they obtained enough evidence to support a conviction. And like Carpenter, it was only through use of CSLI records—which law enforcement utilized as a near perfect surveillance of Petitioner's past movements—that Petitioner was implicated as a suspect—and subsequently convicted.

The only difference between Petitioner's case at bar, and Carpenter's, is that it appears law enforcement took deliberate action to circumvent the perceived time constraints held in *Carpenter.* As a result, law enforcement's CSLI request in Petitioner's case was concluded to not be a search invoking Fourth Amendment protections. The Court of Appeal seemingly approved law enforcement's deliberate side-step of the time constraint in affirming Petitioner's conviction. In seemingly approving law enforcement's action by affirming this conviction, the Court of Appeal erroneously ignored the affirmative ruling of *Carpenter* which stated: "[g]overnment **must** generally obtain a warrant supported by probable cause *before* acquiring such records." *Carpenter,* 585 U.S. __ (slip op., at 18).

In following in the precedent established in *Carpenter,* it appears axiomatic that in Petitioner's case, "an order under Section 2703(d) of the Act is not a permissible mechanism for assessing historical cell-site records." *Carpenter,* 585 U.S. __ (slip op., at 19). The Court—unquestionably advised that—"[b]efore compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant. *Id.* Because a warrant was not obtained in Petitioner's case—as instructed under *Carpenter*—the district court's conviction, affirmed by the Court of Appeal, for the Fourteenth Circuit, must be reversed.

CONCLUSION

Petitioner respectfully requests that this Court reverse the denial regarding the motion to suppress the results of the forensic search. Petitioner requests this reversal asserting that the District Court – whose conviction was affirmed by the Court of Appeal for the Fourteenth Circuit— erred when it failed to acknowledge the *Touset Court's* ruling that *because* prior intelligence was available to Government agents, reasonable suspicion did exist to conduct a forensic search. Petitioner further contends intelligence and information available to

Government agents, not only provides for reasonable suspicion, but further eliminates any judicial second guessing – by providing Government agents with proper intelligence to conduct a proper forensic search of a electronic device.

Additionally, Petitioner respectfully requests that this Court reverse his conviction regarding Bank Fraud, 18 U.S.C. § 1344, Conspiracy to Commit Bank Fraud, 18 U.S.C. § 1349, and Aggravated Identity Theft, 18 U.S.C. § 1028A. Petitioner requests this reversal asserting that the District Court—whose conviction was affirmed by the Court of Appeal for the Fourteenth Circuit—erred when it denyied Petitioner's motion to suppress the results of the cell-site location information data collected. Petitioner contends that in denying the motion to suppress, both the District Court and the Court of Appeal erroneously applied *Carpenter,* 585 U.S. __, as holding that *only* requests of CSLI *in excess* of seven days, or 168 hours, can constitute a search—thus violating an individual's Fourth Amendment expectation of privacy. Petitioner contests that the government's acquisitions of CSLI records containing: [1] three days of cell-site location information; [2] one-hundred cumulative hours of cell-site location information over two weeks; and [3] cell-site location information collected from cell tower dumps **does constitute a search, *thus* violating protections *guaranteed* by the Fourth Amendment.** Petitioner prays this Court to render a decision providing clarification to *Carpenter,* 585 U.S.__, in that all CSLI requests—absent any exception—are searches, invoking fourth amendment protections, regardless of their timeframe.

Respectfully submitted,

Attorneys for Petitioner