No. 10-1011

IN THE

SUPREME COURT OF THE UNITED STATES

HECTOR ESCATON, Petitioner,

v.

UNITED STATES OF AMERICA, Respondent.

On Writ of Certiorari
To The Supreme Court of the United States

BRIEF FOR RESPONDENT

Team #: R2

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

QUESTIONS PRESENTED iv

OPINION BELOW v

CONSTITUTIONAL PROVISIONS AND RULES vi

INTRODUCTION 1

STATEMENT OF THE CASE 3

ARGUMENT 6

I. STANDARD OF REVIEW 6

II. THE FOURTH AMENDMENT OF THE UNITED STATE CONSTITUTION DOES NOT DEMAND REASONABLE SUSPICION TO CONDUCT A FORENSIC SEARCH AT THE BORDER 6

A. The Fourteenth Circuit correctly found that border officials need not develop reasonable suspicion at the outset of a forensic search because Officer Stubbs and Agent Cullen conducted a routine and non-offensive search. 9

B. No Distinction Should be Drawn Between Forensic and Non-Forensic Border Searches, and Such a Holding Would Not Contradict the Justifications behind *Riley v. California* and Its Progeny. 13

C. Even If This Court Crafts a New Rule, Heightening the Suspicion Requirement for Forensic Searches at the International Border, the Application Should Be Limited to Highly Intrusive Searches and Officer Stubbs's Search Was Not Invasive Enough to Trigger This New Standard. 16

III. LAW ENFORCEMENT'S LIMITED REQUESTS FOR HISTORICAL CELL-SITE LOCATION INFORMATION DID NOT AMOUNT TO SEARCHES UNDER THE FOURTH AMENDMENT 16

A. This Court's Restrictions on CSLI Records in *Carpenter* Do Not Extend to the Three-Day Records or the Weekday Records Because They Were Sufficiently Limited and Do Not Elicit the *Carpenter* Court's Privacy Concerns. 17

1. The *Carpenter* majority was predominantly concerned with the amount of time that the CSLI allowed the Government to monitor Carpenter's Movements 18

2. The Three-Day Records and the Weekday Records were sufficiently limited and do not amount to Fourth Amendment searches after *Carpenter*..... 22

B. Any Further Restrictions on CSLI Records Would Unduly Impede Serious Criminal Investigations, Offend Congress's Purpose, and Deviate from this Court's Fourth Amendment Precedent..... 24

C. *Carpenter* Should Not Apply to the Tower Dump Requests Because Tower Dumps Do Not Provide a Comprehensive Record of a Person's Movements..... 28

CONCLUSION 30

TABLE OF AUTHORITIES

Cases

California v. Acevedo,
500 U.S. 565 (1991)……3

California v. Carney,
471 U.S. 386 (1985)……6, 9

Camara v. Municipal Court,
387 U.S. 523 (1967)……

Carpenter v. United States,
138 S. Ct. 2206 (2018)……passim

Cty. of Riverside v. McLaughlin,
500 U.S. 44, 58 (1991)……

Katz v. United States,
389 U.S. 347, 351 (1967)…….

Kyllo v. United States,
533 U.S. 27 (2001)……

New Jersey v. T.L.O.,
469 U.S. 325 (1985)……...

Ornelas v. United States,
517 U.S. 690 (1996)……..

Osborne v. Ohio,
495 U.S. 103 (1990)……..

People v. Simpson,
88 N.Y.S.3d 763 (N.Y. Sup. Ct. 2018)…….

Riley v. California,
134 S. Ct. 2473 (2014)……passim

Sims v. State,
No. PD-0941-17, 2019 WL 208631 (Tex. Crim. App. Jan. 16, 2019)……..

Smith v. Maryland,
442 U.S. 735 (1979)……passim

United States v. 12,200–Ft. Reels of Super 8MM. Film,
413 U.S. 123 (1973)……

United States v. Alfaro-Moncada,
607 F.3d 720 (11th Cir. 2010)……..

United States v. Arnold,
533 F.3d 1003 (9th Cir. 2008)……passim

United States v. Carreon,
872 F.2d 1436 (C.A.10 1989)……

United States v. Cortez–Rocha,
394 F.3d 1115 (9th Cir. 2005)……...

United States v. Cotterman,
709 F.3d 952 (9th Cir. 2013)…….

United States v. Evans,
No. 5:17-CR-39-FL-1, 2018 WL 7051095 (E.D.N.C. Dec. 20, 2018)……..

United States v. Flores-Montano,
541 U.S. 149 (2004)……

United States v. Graham,
824 F.3d 421 (4th Cir. 2016)……

United States v. Jones,
565 U.S. 400 (2012)……passim

United States v. Knotts,
460 U.S. 276 (1983)……

United States v. Kubasiak,
No. 18-CR-120-PP, 2018 WL 4846761 (E.D. Wis. Oct. 5, 2018)……..

United States v. Miller,
425 U.S. 435 (1976)……passim

United States v. Monroe,
No. CR 16-00055 WES, 2018 WL 5717367 (D.R.I. Nov. 1, 2018)…….

United States v. Montoya de Hernandez,
473 U.S. 531 (1985)……

United States v. Muglata,
44 F.3d 1530 (11th Cir. 1995)…….

United States v. Newsome,
475 F.3d 1221 (11th Cir. 2007)……

United States v. Ramsey,
431 U.S. 606 (1977)……..

United States v. Rivas,
157 F.3d 364 (C.A.5 1998)……

United States v. Robles,
45 F.3d 1 (C.A.1 1995)…….

United States v. Romm,
455 F.3d 990 (9th Cir. 2006)…….

United States v. Tirado,
No. 16-CR-168, 2018 WL 3995901, at *2 (E.D. Wis. Aug. 21, 2018)……..

United States v. Touset,
890 F.3d 1227 (11th Cir. 2018)…….

United States v. Vega-Barvo,
729 F.2d 1346 (11th Cir. 1984)…….……

Statutes

STORED COMMUNICATIONS ACT…….passim

ECPA Modernization Act of 2017, S.B. 1657 (2018)……..

Secondary Authorities

Kit Kinports, *Culpability, Deterrence, and the Exclusionary Rule*,
21 WM. & MARY BILL RTS. J. 821 (2013)…….

Albert Gidari, *The Practical Impact of Carpenter v. United States*,
STANFORD L. SCH.: CTR. FOR INTERNET & SOC'Y (Nov. 30, 2017, 4:36 PM)……..

Jennifer Valentino-DeVries, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y TIMES (Dec. 10, 2018)……..

QUESTIONS PRESENTED

1. Under the Fourth Amendment of the United States Constitution, may officers at international borders conduct forensic searches before developing reasonable suspicion?
    a. Did the 14th Circuit Court of Appeals correctly find that forensic border searches require no particularized suspicion at their outset?
    b. Does finding no requirement for particularized suspicion for forensic searches at an international border comport with cases such as *Riley* and its progeny?
    c. Even if this court finds that some forensic searches call for particularized suspicion at the outset, was the search conducted by Officer Stubbs sufficiently limited so as not to require this heightened suspicion?
2. Under the Fourth Amendment of the United States Constitution, may law enforcement request limited periods of CSLI from cell-service providers with a court order?
    a. Does this Court's decision in Carpenter extend to the Three-day Records and the Weekday Records obtained by Agent Hale?
    b. If *Carpenter* does not extend to the present action, should this Court defer to the Legislature or set forth a distinctive rule that limited periods of CSLI can continue to be obtained under the Stored Communications Act?
    c. Does *Carpenter* apply to tower dumps if they don't produce the kind of location monitoring this Court was concerned about?

OPINION BELOW

The United States Court of Appeals for the Fourteenth Circuit issued its opinion on November 2, 2021, and affirmed the ruling below. The opinion and order are recorded at *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment of the United States Constitution provides:

> 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.

INTRODUCTION

This Court should affirm the Fourteenth Circuit's opinion because it correctly held that, under the border exception to the Fourth Amendment of the United States Constitution, searches made at the border are reasonable simply by virtue of the fact that they occur at the border.

Flores-Montano determined that the government's interest in preventing the entry of unwanted people and contraband is at its zenith at the international border. Therefore, so long as a search is not offensive or non-routine, no reasonable suspicion is required at its outset.

However, even if this court determines that it should fashion a new standard to the border exception, the search conducted by Officer Stubbs and Agent Cullen was sufficiently limited to not call for reasonable suspicion at its outset.

The Fourteenth Circuit correctly held that Agent Hale's requests for cell-site location information ("CSLI") were not searches under the Fourth Amendment. *Carpenter v. United States* is the first decision to significantly restrict law enforcement's use of CSLI. However, it did not go so far as to restrict the type of CSLI requests made by Agent Hale.

Carpenter held that the Government must obtain a warrant to compel production of more than one week's worth of CSLI from third-party cell service providers. The *Carpenter* Court expressly refused to rule on more limited periods of CSLI, including tower dumps, likely because this Court recognized that individuals do not have reasonable expectation of privacy in all CSLI. In a slim 5-4 majority, *Carpenter* also declined to extend pertinent, longstanding precedent from *Smith v. Maryland* and *United States v. Miller* to the CSLI records at issue because the requests in *Carpenter* were so extensive as to provide the Government with an "intimate window into a person's life." *Carpenter* placed heavy emphasis on the potential intrusiveness of CSLI and indicated that CSLI records can rise to a level in which individuals

have a reasonable expectation of privacy in them. However, the CSLI requests in the present action fall short.

The Three Day Records and Weekday Records are sufficiently limited in scope to information that Appellant has no reasonable expectation of privacy in them. Unlike the CSLI in *Carpenter*, both records did not produce enough information to give law enforcement an "intimate window" into Appellant's private life. Because *Carpenter* is primarily concerned with the intrusiveness of extended periods of CSLI, the requests here fall outside of *Carpenter's* restrictions. *Carpenter* also does not apply to the tower dumps because they did not track Petitioner's location; rather, the tower dumps provided Petitioner's location at a specific place at a particular time.

For these reasons explained in detail below, the United States of America asks the Court to affirm the Fourteenth Circuit's decision.

STATEMENT OF THE CASE

ATM Skimming

During October of 2018, Mariposa Bank and its customers in both the cities of Sweetwater and Escalante fell victim to a complex, high tech version of ATM skimming. (R. at 3). Hector Escaton (hereinafter "Petitioner") had cut open Mariposa Bank ATMs and infected the machine with malware through its USB port. (R. at 3). This malware took the information

from customers who had used the infected ATM terminals. (R. at 3). Petitioner could then use this stolen information to create fake credit and debit card accounts - even permitting Petitioner to directly withdraw funds from ATMs. (R. at 3).

After ATMs at eight Mariposa Bank branches in Sweetwater and Escalante were vandalized in October of 2018, the FBI initiated an investigation. (R. at 4). Mariposa Bank conducted its own internal investigation and reported its findings to the FBI. (R. at 4).

Sweetwater and Escalante are neighboring cities in West Texas. (Affidavit in Support of an Application for 2703(d) Court Order). Sweetwater is a densely populated, large city while Escalante is a smaller, suburban town. (Aff. ¶ 11-12). Mariposa's internal investigation revealed that it had suffered around $50,000 of losses in just the month of October from direct withdrawals and false account creation resulting from the ATM skimming. (R. at 4).

FBI Special Agent, Catherine Hale, was given this information almost a year later and was limited to only a few tools that would allow her to locate and track as suspect. (R. at 2-3). Agent Hale first received surveillance photographs of a man in a black sweatshirt near three of the Mariposa ATMS. (R. at 4). Then, she requested three tower dumps, which provide list of every phone number that connected a tower at a particular time, under the Stored Communications Act ("SCA") to get the cell numbers of those phones used around the three ATMs thirty minutes before and after the man in the black sweatshirt was at the ATMs. (R. at 4). Escaton's phone number, which was revealed to law enforcement during the border search, matched one of the numbers generated from the three tower dumps. (R. at 5).

This furthered Agent Hale's investigation and allowed her to make a limited, particularized request for three days of CSLI records ("Three-day Records") from Escaton's wireless provider, Delos Wireless. (R. at 5). A federal magistrate judge issued an order

directing Delos Wireless to disclose Escaton's CSLI from October 11, 2018 through October 13, 2018. (R. at 5). Because Mariposa Bank branch manager Maeve Millay discovered the ATM tampering on October 13 at the Boswell Street branch two days after the ATMs were service, Officer Hale was able to limit this request to a 72-hour window. (Aff. ¶ 18). This information showed Escaton's cell phone in the area of the Sweetwater Boswell Branch ATM on October 12. (R. at 5). It did not place him in Escalante. (R. at 5).

To see if Escaton was also involved in the ATM skimming in Escalante, Agent Hale also requested two weeks of weekday CSLI records ("Weekday Records") between October 1 and 12, during business hours from 8 a.m. to 6 p.m. amounting to 100 hours of CSLI. The Mariposa Bank ATMs in Sweetwater and Escalante are inaccessible outside of working hours between 8 a.m. and 6 p.m., as the ATMs are located in locked bank branches. (Aff. ¶ 17). There have also been no reports or surveillance evidence showing that the bank branches were unauthorizedly accessed outside of those hours. (Aff. ¶ 17).

Unlike the Three-day records, this request was not just for Escaton but also for the "Delores" identified on the paper note in the laptop. (R. at 5). Agent Hale wanted to get information on whether she was involved in abetting Escaton's scheme. (R. at 5). These records revealed "Delores" as Delores Abernathy, who had been previously convicted for ATM skimming, and showed that Escaton was with Delores during early October in the area of the three defrauded Escalante ATMs. (R. at 5).

Because Sweetwater is so densely populated and has many tall buildings, there is a significantly large number of cell towers so that the tall buildings do not block access to cell service. (Aff. ¶ 11). The Delos Wireless cell towers in Sweetwater often capture CSLI when cell phones are within fifty feet of the towers, which can be as accurate as GPS systems when

tracking location. (Aff. ¶ 11). Escalante, however, contains few Delos Wireless cell towers and CSLI is only accurate when cell phones are within 1000 feet of the individual. (Aff. ¶ 12).

The Border Search

On September 25, 2019, Petitioner re-entered the United States from Mexico. (R. at 2). At the West Texas border checkpoint, CBP Officer Ashley Stubbs conducted a routine border search of Petitioner's vehicle. (R. at 2). During this search, Officer Stubbs discovered one iPhone, one laptop, three external hard drives, and four USB devices.

After placing the iPhone on airplane mode, and confirming that the laptop was not connected to wireless internet, Officer Stubbs began to search each device. (RT 3.) Officer Stubbs found that, while none of the devices were password protected, some of the internal folders were. (RT 3.) In addition, Officer Stubbs found a paper note on the laptop which read, "Call Delores (201) 181-0981 $$$."

A forensic program scanned the laptop, and Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen found not only documents containing individuals' bank account numbers and pins, but also traces of malware. (RT 3.)

CBP notified the Federal Bureau of Investigation (FBI). (RT 3.)

Procedural Posture

Petitioner moved to suppress the evidence from both the forensic border search and the CSLI requests, but the district court denied the motion. (R. at 2). A jury convicted Petitioner of bank fraud, 18 U.S.C. § 1344, conspiracy to commit bank fraud, §1349, and aggravated identity theft, 18 U.S.C. § 1028A. (R. at 2). Petitioner has appealed his convictions on the grounds that the district court erred in denying his motion to suppress. (R. at 2).

ARGUMENT

I. STANDARD OF REVIEW

Motions to suppress involve mixed questions of fact and law, therefore, the Fourteenth Circuit's legal conclusions are reviewed under the de novo standard and its factual determinations are reviewed for clear error. *United States v. Muglata*, 44 F.3d 1530, 1536 (11th Cir. 1995); *United States v. Cotterman*, 709 F.3d 952, 968 (9th Cir. 2013) (en banc) (citing *Ornelas v. United States*, 517 U.S. 690, 699 (1996)). Upon review, all facts are construed "in the light most favorable to the prevailing party below." *United States v. Newsome*, 475 F.3d 1221, 1224 (11th Cir. 2007) (internal quotation marks omitted). Additionally, "[t]he individual challenging the search bears the burdens of proof and persuasion." *Id.* (internal quotation marks omitted).

II. THE FOURTH AMENDMENT OF THE UNITED STATES CONSTITUTION DOES NOT DEMAN REASONABLE SUSPICION TO CONDUCT A FORENSIC SEARCH AT AN INTERNATIONAL BORDER.

This Court should affirm the Fourteenth Circuit Court of Appeals and hold that the District Court properly denied Petitioner's motion to suppress evidence. The Fourth Amendment of the United State Constitution functions to safeguard "the privacy and security of individuals against arbitrary invasions by government officials" by requiring, except in "certain carefully defined classes of cases," a magistrate's prior authorization even where "[p]robable cause in the criminal law sense is not required." *Camara v. Municipal Court*, 387 U.S. 523, 528 (1967). One such carefully defined class of cases which does not require a magistrate's prior authorization is searches conducted at the international border. *See United States v. Ramsey*, 431 U.S. 606 (1977).

"At the border, an individual has a lesser expectation of privacy, the government has a greater interest in searching, and the balance between the interests of the government and the privacy right of the individual is struck more favorably to the government." *United States v. Alfaro-Moncada*, 607 F.3d 720, 728 (11th Cir. 2010). Thus, the inception of a forensic search need not be predicated by an officer's reasonable suspicion. Even considering this Court's recent holding in *Riley v. California*, which set new precedent protecting an individual's privacy in their cell phone during searches incident to arrest, the border search exception remains firm because, it rests on different considerations and different rules of constitutional law from domestic regulations. 134 S. Ct. 2473, 2484 (2014); s*ee also United States v. 12,200–Ft. Reels of Super 8MM. Film,* 413 U.S. 123, 124–25 (1973). Finally, even if this Court wishes to increase individual protections of privacy at the international border, only when forensic searches are time consuming, are conducted off site, and divulge information that would not otherwise be found by a manual search should the Fourth Amendment require reasonable suspicion at the outset. *United States v. Arnold*, 533 F.3d 1003 (9th Cir. 2008); *Cotterman*, 709 F.3d at 952.

A. The Fourteenth Circuit Correctly Found that Border Officials Need Not Develop Reasonable Suspicion at the Outset of a Forensic Search Because Officer Stubbs and Agent Cullen Conducted a Routine and Non-Offensive Search.

The Fourth Amendment protects the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. U.S. CONST. amend. IV. "Because the Fourth Amendment expressly prohibits only unreasonable warrantless searches, it patently incorporates a balancing test, weighing in one measure the level of intrusion into individual privacy and in the other the public interest to be served." *Alfaro-Moncada*, 607 F.3d at 727.

Even though it does involve weighing individual privacy and public interests, "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior." *Id.* at 727–28.

> That searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should by now, require no extended demonstration.

Ramsey, 431 U.S. at 616. However, this exception to the warrant requirement is not unfettered - this Court has distinguished searches conducted at the border between those that are particularly offensive and those which are not. *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). Although the Supreme court has rejected a balancing test based on a "routine" and "non-routine" framework, these terms are often applied when analyzing whether a search has been conducted in a particularly offensive manner. *See United States v. Cortez–Rocha,* 394 F.3d 1115, 1122 (9th Cir. 2005). Routine, non-offensive searches do not require reasonable suspicion, while searches which have been determined to be non-routine and particularly offensive do. *Montoya de Hernandez*, 473 U.S. at 538.

Most searches conducted at the border are considered routine and non-offensive, even if the individuals subjected to the search would receive much more protection in the interior. For instance, the very core of the Fourth Amendment is the right of a person to retreat into his own home to be free from unreasonable government intrusion. *Kyllo v. United States*, 533 U.S. 27, 31 (2001). However, in *Alfaro-Moncada*, the Eleventh Circuit found that the search of a crew member's home on a cargo boat did not violate the Fourth Amendment, despite lacking any form of heightened suspicion at the outset of the search. 607 F.3d at 730. The court even acknowledged that the entry of the home by government officials is the chief evil against which the wording of the Fourth Amendment is directed, but found that a home on a boat can be used

as a means to transport into this country contraband or weapons that threaten national security. *Id.* at 729-30. Thus, simply by virtue of the fact that they occur at the border, routine, non-offensive searches are reasonable per se. *See Ramsey*, 431 U.S. at 619.

On the other hand, courts will only consider searches non-routine and offensive if they involve intrusive searches of a person's body or destruction of personal property. These instances are typically determined on a case by case basis; what is reasonable still depends upon all of the circumstances surrounding the search or seizure and the nature of the search or seizure itself. *New Jersey v. T.L.O.*, 469 U.S. 325, 337-342 (1985). For example, in *Montoya de Hernandez*, upon the defendant's arrival at Los Angeles International Airport, customs officials detained the defendant when, after examination of her the contents of her luggage and questioning by the officials, she was suspected of being a "balloon swallower," and was subjected to at least one strip search. 473 U.S. at 540.[1]

The defendant was detained for almost 16 hours before the officials sought a court order authorizing a pregnancy test, an x ray, and a rectal examination. *Id* at p. ??? During those 16 hours she was given the option of returning to Colombia on the next available flight, agreeing to an x ray, or remaining in detention until she produced a monitored bowel movement. *Id* at p. ??? The court held that that the officer acted in a way beyond the scope of a routine customs search and inspection, and therefore, the Fourth Amendment required the officers to reasonably suspect the defendant of smuggling contraband in her alimentary canal before the search began. *Id*. at 541.[2]

---

[1] Although the facts in the opinion of this case discuss a single strip search, the dissent mentions not just two strip searches, but also a much longer detention. (CITE)

[2] Similarly, destruction of property has been held to require heightened suspicion. *See United States v. Rivas*, 157 F.3d 364 (C.A.5 1998) (drilling into body of trailer required reasonable suspicion); *United States v. Robles*, 45 F.3d 1 (C.A.1 1995) (drilling into machine part required reasonable suspicion); *United States v. Carreon*, 872 F.2d 1436 (C.A.10 1989) (drilling into camper required reasonable suspicion).

Here, Officer Stubbs, upon finding Petitioner's iPhone, laptop, three external hard drives, and four USB drives, first confirmed that they were disconnected from the internet, and then manually searched the devices without any assistance. (R. at 2). After returning the iPhone to Petitioner, Officer Stubbs then sought the assistance of ICE Agent Cullen and her forensic software. (R. at 3). This process only took a few hours, revealed only documents saved on the device and evidence of a malware program. (R. at 3). This search lasted a relatively short period of time, did not destroy any of Petitioner's personal property, and did not subject Petitioner to exposure of any intimate body parts. By no respect did this search exceed what is routine. Indeed, nothing about Officer Stubbs' or Agent Cullens' actions could be colored as "offensive."

While the actions of Officer Stubbs and Agent Cullens may have violated Petitioner's Fourth Amendment rights had they taken place in the interior, fell well within what is routine and non-offensive for a border search. Therefore, this Court should find that reasonable suspicion was not required at the outset of the forensic search of Petitioner's laptop, hard drives, and USB devices, and this Court should affirm the holding of the Fourteenth Circuit Court of Appeals.

B. No Distinction Should be Drawn Between Forensic and Non-Forensic Border Searches, and Such a Holding Would Not Contradict the Justifications Behind *Riley v. California* and Its Progeny.

In *Riley v. California*, this Court found that the police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested. 134 S. Ct. at ???. The court discussed extensively the implications of new technology on the criminal justice system, however limited its finding to the search incident to arrest exception to the warrant requirement, as a phone search would not typically support the justification for a search incident to arrest. *Id.*

In finding that officers may not generally search the contents of an arrestee's phone, the court acknowledged that cell phones are such a pervasive and insistent part of daily life, a "proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Id.* at 2484. In balancing this somewhat unprecedented interest of individual privacy against that of the government's interests, the court explained its logic: rather than requiring a "case-by-case adjudication," the question instead is whether application of the search incident to arrest doctrine to this particular category of effects would "*untether the rule from the justifications underlying the...exception*." *Id.* at 2485 (emphasis added) (finding that the justification behind a search incident to arrest relates only to the safety of officers and the need to prevent the destruction of evidence, the court found no reason to permit such intrusive searches which would not advance those concerns) The court found the concerns of "harm to officers and destruction of evidence"—did not "ha[ve] much force with respect to digital content on cell phones," *United States v. Touset*, 890 F.3d 1227, 1235 (11th Cir. 2018). Notably, the court limited the effect of its holding, expressly stating that other case-specific exceptions may still justify a warrantless search of a particular phone. *Riley*, 134 S. Ct. at 2494.

The justification for border searches, on the other hand, carries much more force with forensic searches. Indeed, "digital" contraband poses the same exact "risk" of unlawful entry at the border as its physical counterpart. *Touset*, 890 F.3d at 1235. If anything, the advent of sophisticated technological means for concealing illicit materials only heightens the need of the government to search property at the border unencumbered by judicial second-guessing. *Id.* at 1235.

> At the border, customs officials have more than merely an investigative law enforcement role. They are also charged, along with immigration officials, with protecting this Nation from entrants who may bring anything harmful into this country, whether that be communicable diseases, narcotics, or explosives.

Montoya de Hernandez, 473 U.S. at 544. Due to this justification, the limits to searches at the border have historically considered only the "personal indignity" of a search, not its extensiveness. *United States v. Vega-Barvo*, 729 F.2d 1346, 1349 (11th Cir. 1984). The courts have been similarly unwilling to distinguish between different kinds of property at the border. *Touset*, 890 F.3d at 1233. Moreover, the "readily mobile" characteristic of technology and its capacity to contain the same illicit materials that the government has attempted to exclude at our borders for years leans in favor of the exceptions justification rather than against it. *See California v. Carney*, 471 U.S. 386, (1985) (finding that officers may enter a mobile home with less suspicion than that required for a typical home due to its "readily mobile" characteristics and the reduced expectation of privacy in a vehicle); *see also Arnold*, 533 F.3d at 1009–10.

The justification behind the border search exception to the warrant requirement of the Fourth Amendment relies upon Congress' broad power to prevent prohibited articles from entry. U.S. Const. art. I, § 8, cl. 1. Certainly, a primary purpose of the border exception relates to the government's interest in "stamping out" criminal activity at its own borders. *See Osborne v. Ohio*, 495 U.S. 103, (1990); *Touset*, 890 F.3d at 1232. It is unquestionable that criminals utilize technology to transport illicit materials - including items like stolen bank account numbers and pins - across the United States border, and Petitioner is no exception. (R. at 3). This falls squarely within the type of action border searches have been utilized to prevent since its inception.

The transportation of contraband across the border is more than just "tethered" to the justification of the border search exception - it is at the heart of it. Thus, holding that reasonable suspicion is not required at the outset of a routine, non-offensive border search would be in line with the logic of *Riley* and its progeny.

C. Even If This Court Crafts a New Rule, Heightening the Suspicion Requirement for Forensic Searches at the International Border, the Application Should Be Limited to Highly Intrusive Searches and Officer Stubbs's Search Was Not Invasive Enough to Trigger This New Standard.

"The plenary authority of the Federal Government to conduct searches and inspections of persons and merchandise crossing our nation's borders is well-established and extensive; control of the border is a fundamental principle of sovereignty." *United States v. Flores-Montano*, 541 U.S. 149, 153 (2004). Other than considering "intrusive searches of the person," the Supreme Court has suggested, "that some searches of property are so destructive as to require" particularized suspicion - but has hesitated to limit the Federal Government's powers to conduct searches at the border.[3] *Id.* at 155-56.

When forensic searches are conducted in a limited manner at the border, they are not so intrusive or destructive as to demand reasonable suspicion at the outset. In *United States v. Romm*, 455 F.3d 990 (9th Cir. 2006), when border agents told the defendant they needed to search his laptop for illegal images, the defendant did not protest. ICE conducted a preliminary forensic analysis of the hard drive in the defendant's laptop and discovered ten images of child pornography. *Id.* at 994-95. The court found that the "routine" border search of the defendant's laptop was reasonable regardless of where, when, or how the pornography had been obtained. *Id.* at 997. Similarly, precedent does not support a finding that a search which occurs in an otherwise ordinary manner, is "particularly offensive" simply due to the storage capacity of the object being searched. *See California v. Acevedo,* 500 U.S. 565, 576, (1991). When there is no basis in the record to support the contention that the manner in which a search occurred was

[3] Courts have expressly repudiated the "least restrictive means test" in the border search context. *See United States v. Cortez-Rocha*, 394 F.3d 1115, 1122 (9th Cir. 2005) (refusing to craft a least restrictive means test for border control vehicle searches, and equally refusing to tie the hands of border control officers in completion of their duties).

"particularly offensive" in light of other searches allowed by the Supreme Court, the actions of the agents will be found lawful. *Arnold*, 533 F.3d at 1010.

Only when time consuming forensic searches are conducted off site and divulge information that would not otherwise be found by a manual search will the courts find that reasonable suspicion is required at the outset. The court in *Cotterman* considered a scenario in which border agents seized a laptop at the U.S.-Mexico based in part on the defendant's fifteen-year-old conviction for child molestation. (CITE??) The initial search at the border turned up no incriminating material. (CITE??) Only after Cotterman's laptop was shipped almost 170 miles away and subjected to a comprehensive forensic examination were images of child pornography discovered - images that seemingly had been deleted from the computer's memory. *Id.* at 962-63. Moving the laptop to a specialized lab at a distant location highlighted that the search undertaken there was an extensive one, but more importantly, the court found that the comprehensive and intrusive nature of a forensic examination triggered the requirement of reasonable suspicion. *Id.* at 962-63. The court concluded stating, that although past decisions like those in *Romm* and *Arnold* had expressed broad powers of the Federal Government to conduct searches at the border, this case was not so simple a search as to permit a suspicionless forensic examination. *Id.* at 960 n. 6. The court also provided guidance, and explained that the Fourth Amendment reasonableness requirement called for officers to make commonsense differentiations between simple reviews of files on an electronic device and the application of computer software to analyze a hard drive - utilizing the latter only when the agents possess a "particularized and objective basis for suspecting the person stopped of criminal activity." *Id.* at 967.

Here, Officer Stubbs began a routine search in compliance with CBP directives by placing the iPhone on airplane mode and ensuring that the laptop was disconnected from wireless internet before manually searching the device. (R. at 2; Dir. No. 049A, 5.1.2). From there, Agent Cullen conducted what CBP classifies as a "basic" forensic search: although utilizing external equipment, Agent Cullen employed the forensic search software merely to inspect only the password locked files and programs installed on the devices. (R. at 2-3; Dir. No. 049A, 5.1.3-5.1.4, 5.3.1, 5.3.4). Agent Cullen did not access internet searches, internet history, or make any attempt to find previously deleted documents. (R. at 2-3). Officer Stubbs and Agent Cullen, unlike the border officers in *Cotterman*, did not unduly prolong their search, did not remove the devices to a distant secondary location, and did not use the forensic search program to access anything that could not be found by a skilled agent conducting a manual search.

Even if this Court wishes to impose a new standard of reasonable suspicion for advanced forensic searches at the border, Officer Stubbs and Agent Cullen conducted a reasonably limited and basic forensic search of Petitioner's laptop. Because there exists no factual basis in the record to support the contention that the manner in which a search occurred was "particularly offensive" in light of other searches upheld by the Supreme Court or the Circuit Courts, the actions of the agents should be found lawful.

III. LAW ENFORCEMENT'S LIMITED REQUESTS FOR HISTORICAL CELL-SITE LOCATION INFORMATION DID NOT AMOUNT TO SEARCHES UNDER THE FOURTH AMENDMENT.

This Court should affirm the Fourteenth Circuit Court of Appeals and hold that law enforcement's requests for cell-site location information ("CSLI") did not violate Petitioner's Fourth Amendment rights. The Fourth Amendment prohibits "unreasonable searches and seizures" and requires the Government to obtain warrants supported by probable cause before

conducting a "Fourth Amendment search," U.S. CONST. amend. IV, or a search that is so intrusive that it violates a person's reasonable expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 351 (1967).

Before this Court decided *Carpenter v. United States*, 138 S. Ct. 2206 (2018), law enforcement could obtain extended periods of CSLI from cell-service providers without a warrant by offering "specific and articulable facts showing that there are reasonable grounds to believe" that the records "are relevant and material to an ongoing investigation." Section 2703(d) of the Stored Communications Act [hereinafter SCA]. Now, after *Carpenter*, law enforcement is required to obtain a warrant before compelling seven or more days of CSLI because individuals have a reasonable expectation of privacy in extended periods of location monitoring as captured by CSLI. 138 S. Ct. at 2221.

A. This Court's Restrictions on CSLI Records in *Carpenter* Do Not Extend to the Three-Day Records or the Weekday Records Because They Were Sufficiently Limited and Do Not Elicit the *Carpenter* Court's Privacy Concerns.

In *Carpenter*, by a 5-to-4 majority, the Court held that the Government may not compel production, without first obtaining a search warrant, of more than one week's worth of CSLI from third-party cell phone service providers. *Id.* The Court declined to say whether there was "a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny." *Id.* at 2217 n. 3.

In *Carpenter*, the Government requested two SCA-orders; one compelling Sprint to provide seven days of the defendant's historical CSLI and another compelling a different provider to disclose another 127 days of CSLI. *Id.* at 2212. The CSLI production amounted to 12,898 location points cataloging the defendant's movements and, as this Court describes, an "all-encompassing record of [Carpenter's] whereabouts." *Id.* at 2217. This Court recognized that

prolonged CSLI requests could potentially allow law enforcement to backtrack a suspect "every moment of every day for five years" because wireless carriers maintain those records "for up to five years." *Id.* at 2217-18.

However, not all CSLI requests are as expansive as the ones in *Carpenter*, and as *Carpenter* notes, "[it] is certainly not to say that all orders compelling the production of documents will require a showing of probable cause." *Id.* at 2222. Just like "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," *Carpenter*, 138 S. Ct. at 2215 (quoting *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring)), requests for longer periods of CSLI implicate the Fourth Amendment.

1. The *Carpenter* Majority Was Predominantly Concerned with the Amount of Time that the CSLI Allowed the Government to Monitor Carpenter's Movements.

In *Carpenter*, the Court proscribed warrantless requests for CSLI records that allow law enforcement to "chronicle a person's past movements *over an extended period of time*." 138 S. Ct. at 2221. The *Carpenter* majority dedicated most of its analysis to privacy concerns that emerge when an individual is tracked for longer periods of time, first by distinguishing short-term public tracking approved in previous cases from long-term surveillance of a person's every move. *See id.* at 2215; *see also United States v. Tirado*, No. 16-CR-168, 2018 WL 3995901, at *2 (E.D. Wis. Aug. 21, 2018). *Carpenter* also emphasizes the duration of personal information disclosure; "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement . . . for a very long period." 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 430).

Further, *Carpenter* critically relied on *Jones* to bring CSLI under Fourth Amendment protection. *Id.* at 2215. The Court analogized extended periods of CSLI to the "longer term GPS monitoring" in *Jones*. *Id.* This Court also derived its holding from Justice Alito's so-called

"Mosaic theory," which stated that individuals have a reasonable expectation of privacy in information that allows law enforcement to "secretly monitor and catalogue every single movement of an individual's car for a very long period." *Jones*, 565 U.S. at 430 (Alito, J., concurring). Like *Carpenter*, *Jones* was predominantly concerned with the length of location monitoring. *Id.*

In addition to placing significant weight on the duration of the CSLI records in *Carpenter*, this Court expressly refused to hold that historical CSLI requests require probable cause in all instances. 128 S. Ct. at 2221. The narrow holding indicates the persuasiveness of prior precedent distinguishing longer periods of tracking from shorter periods, as well as this Court's recognition that limited CSLI is constitutionally different than the CSLI in *Carpenter*. The Court drew an implied distinction between the CSLI requests in *Carpenter* and more limited CSLI requests when it considerably analyzed the general nature of all CSLI, but only held that a week's worth of CSLI or more requires a warrant. *Id.* The Court left for another day the full interpretation of the Fourth Amendment with respect to all types of CSLI requests, but provided important guidance as to the privacy concerns that are raised when law enforcement is able to track an individual's movement for a substantial period of time.

If the *Carpenter* Court required warrants for limited CSLI requests, it would have ruled on CSLI as a whole, but this Court expressly declined the opportunity to do so. *Id.* Instead, law enforcement is left without necessary guidance as to whether short-term CSLI is still constitutionally attainable. By expressly excluding limited periods of CSLI from the holding in the leading Supreme Court case on CSLI, *Carpenter* initiated a situation where magistrate judges will inconsistently suppress evidence obtained from limited, court-ordered CSLI records.

Already, the lower courts that have adjudicated Post-*Carpenter* requests for less than a week's worth of CSLI have inconsistently interpreted *Carpenter*.[4]

After *Carpenter*, it is possible that prosecutors will encourage law enforcement to err on the side of caution and obtain warrants before any CSLI request, no matter how limited. However, this fails to conform with this Court's longstanding criminal procedure jurisprudence on deterrence and the good faith doctrine. *See generally* Kit Kinports, *Culpability, Deterrence, and the Exclusionary Rule*, 21 WM. & MARY BILL RTS. J. 821 (2013) (describing the Court's recognition of the good-faith exception and role of deterrence in criminal procedure). Not only is law enforcement inadequately deterred, the top four major wireless carriers have continued to produce court-ordered CSLI records, even after the enormous amount of attention drawn to the *Carpenter* oral arguments at the end of 2017. *See* Albert Gidari, *The Practical Impact of Carpenter v. United States*, STANFORD L. SCH.: CTR. FOR INTERNET & SOC'Y (Nov. 30, 2017, 4:36 PM), http://cyberlaw.stanford.edu/blog/2017/11/practical-impact-carpenter-v-united-states.

2. The Three-Day Records and the Weekday Records were sufficiently limited and do not amount to Fourth Amendment searches under *Carpenter*.

Unlike *Carpenter*, this is not a "rare case where the suspect has a legitimate privacy interest in records held by a third party." 138 S. Ct. at 2222 ("The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations."). The CSLI records obtained by Agent Hale are significantly different than those in *Carpenter* because Agent Hale made particularized requests for less than a week's worth of CSLI to place Appellant at the Mariposa banks at the time of the frauds. Fortunately, Agent Hale's investigation, along with her

[4] *Compare People v. Simpson*, 88 N.Y.S.3d 763, 771 (N.Y. Sup. Ct. 2018) (holding that *Carpenter* applies to less than a week's worth of CSLI), *and Sims v. State*, No. PD-0941-17, 2019 WL 208631, at *8 (Tex. Crim. App. Jan. 16, 2019) (declining to extend *Carpenter* to less than a day's worth of CSLI).

sources and evidentiary materials, allowed her to tailor the CSLI requests to small windows of time. (Affidavit in Support of an Application for 2703(d) Court Order).

Unlike the CSLI in *Carpenter*, neither the Weekday Records nor the Three-day Records were extensive enough to provide an "intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* at 2217. The Three-day Records merely allowed Agent Hale to affirm or deny her major investigative leads that Appellant was at the specific Mariposa banks during the specific three-day timeframe given by the bank manager. Indeed, it was possible that Appellant was innocent and not near the location of the banks at the time of the frauds, which would have ended any further use of the CSLI records.

Although the Three-day Records potentially allowed Agent Hale to track Appellant's movements in and out of private places, such as his home, they were insufficient as to provide an "intimate window" into Appellant's personal life or significant impressions of Appellant's "familial, political, professional, religious, and sexual associations." An individual's location during any three-day span may reveal, at the most, scare sensitive information, in stark contrast to the location data provided by the CSLI in *Carpenter*.

The Weekday Records also fall outside the privacy concerns in *Carpenter*. The privacy interest in tracking an individual during business hours on weekdays more closely resembles that in *United States v. Knotts*. 460 U.S. 276, 284 (1983) (holding that concealing a tracking device in chemicals purchased by a suspect and monitoring the transport of the chemicals by vehicle outside private premises is not a Fourth Amendment search). The *Knotts* Court reasoned that when a suspect voluntarily shares his vehicle's location with the public by driving it on "public thoroughfares," no reasonable expectation of privacy of his movements exists. *Id.* at 281.

Visual surveillance from public places would have revealed the same information, and the fact that the officers in *Knotts* used a beeper does not elevate the tool to Fourth Amendment scrutiny. *Id.* at 282.

Similarly, here, Appellant has no reasonable expectation of privacy in his public, daytime movements from bank to bank, likely using "public thoroughfares." The Weekday Records were also limited to the banks' hours of operation, which is the only time anyone can access or has accessed the Mariposa Bank ATMs, (Aff. ¶ 17), and law enforcement could have obtained the same information if they had officers conducting visual surveillance at those banks. However, this would have been far more costly, and under the same reasoning as this Court in *Knotts*, it should not elevate the Weekday Records to Fourth Amendment scrutiny.

Although the Weekday Records span two weeks, they amount to 100 hours of CSLI and do not reveal the one week or more of location data protected by *Carpenter*. And this was not a "deliberate attempt to side-step *Carpenter*," (R. at 16), but rather it was an attempt to limit on the potential intrusiveness on Appellant's location tracking. This was part of law enforcement's effort to strictly tailor the location data to either place Appellant at the banks at the time of the frauds or not. Moreover, the Mariposa Bank ATMs are inaccessible outside of those business hours and there are no reports or surveillance evidence showing that they were unauthorizedly accessed outside of working hours. (Aff. ¶ 17). This was not a "creative way to get around Fourth Amendment rights" and "circumvent Carpenter," (R. at 16); instead, it serves as a prime example of the kind of particularized CSLI request where *Carpenter's* privacy concerns are significantly diminished.

The *Carpenter* Court also expressed concern over law enforcement's ability to track everyone's location, not just Carpenter's. 138 S. Ct. at 2219. Here, however, the Three-day

Records were limited to one suspect and the Weekday Records were limited to that same suspect and the suspected abettor in the fraud scheme, Dolores Abernathy. (R. at 5). Agent Hale limited the first Three-day Records request to Appellant, and only included Ms. Abernathy in the second request for Weekday Records because the Three-day Records placed Appellant in Sweetwater, but not Escalante, and Ms. Abernathy was the secondary suspect. (R. at 5). The Three-day Records were either too limited or the varying degrees of cell-tower accuracy in Sweetwater and Escalante allowed just the Sweetwater towers to pick up Appellant's location during the three-day span. It is evident that Agent Hale took significant steps to gather only the information necessary for the investigation because she confined her first request too much that a second limited request was required to locate Appellant in Escalante during the relevant time period.

Carpenter emphasizes the uniquely intrusive nature of CSLI, but just because CSLI is robust does not mean that it is always accurate or reliable. 138 S. Ct. at 2225 (Kennedy, J., dissenting) ("In rural areas cell-site records can be up to 40 times more imprecise."). Indeed, here, the accuracy of CSLI in Escalante is 50 times more imprecise than its West Texas neighboring city, Sweetwater. (Aff. ¶ 11-12). Sweetwater's cell-towers often capture CSLI within 50 feet of a phone's location while Escalante's cell-towers tend to only capture accurate CSLI within 1000 feet of the phone. (Aff. ¶ 11-12). Cell-site location data can vary immensely depending upon the accuracy and reliability of the cell-towers, and many suburban cities, like Escalante, will produce lower volumes of location points, especially when CSLI requests are for short periods of time.

The Three-day Records, which provided just 72 hours of CSLI to locate Appellant in Sweetwater, generated more location points per hour than the Weekday Records, which provided 100 hours of CSLI to locate Appellant in Sweetwater, due to the significant differences between

the two cities' cell-tower infrastructure. Thus, both sets of CSLI records likely produced comparable numbers of location points. They were also certainly lower than the 12,898 location points in *Carpenter* that allowed law enforcement to catalog Carpenter's movements for an unreasonable amount of time.

Although the cell-towers in Sweetwater can sometimes provide more accurate location information than GPS tracking, (Aff. ¶ 11), this is atypical of CSLI because cell-towers do not continually track an individual like GPS does, and as a result, CSLI often only reveals intermittent location tracking. Sweetwater is also a uniquely large, densely populated city in Texas where many small cell-towers are set up, in addition to larger cell-towers, to enhance cell service that is blocked by the many tall buildings in Sweetwater. (Aff. ¶ 11). Appellant's location data derived from the Three-day Records while Appellant was in Sweetwater was likely very minimal because although Sweetwater's cell-towers are uniquely precise, Appellant was only in Sweetwater for one of the three days his location was tracked. (R. at 5).

In summary, the *Carpenter* Court was drawn to its narrow holding after analyzing the nature of extended CSLI records and determining that individuals have a reasonable expectation of privacy in the "pervasive tracking" of their location. More limited periods of CSLI do not implicate the same privacy concerns, which is likely why the Court intentionally directed its holding to seven days or more of CSLI after completing its analysis on CSLI generally. Therefore, the Three-day Records and the Weekday Records are beyond the scope of *Carpenter*.

B. Any Further Restrictions on CSLI Records Would Unduly Impede Serious Criminal Investigations, Offend Congress's Purpose, and Deviate from this Court's Fourth Amendment Precedent.

Carpenter's ruling should be nothing more than the outer bound of this Court's restrictions on CSLI usage by law enforcement. Further limitations on an effective investigatory tool that

does not prompt the privacy concerns in *Carpenter* would strike an improper balance between liberty and security and inhibit law enforcement beyond what is reasonably necessary. *Carpenter* already addressed privacy concerns with respect to CSLI and arguably went further. 138 S. Ct. at 2223 (Kennedy, J., dissenting) (stating that the majority's new rule "places undue restrictions on the lawful and necessary enforcement powers exercised not only by the Federal Government, but also by law enforcement in every State and locality throughout the Nation."). Notably, the *Carpenter* majority recognized the risks of further extending its holding to limited periods of CSLI. *Id.* at 2220 ("[T]he Court must tread carefully ... to ensure we do not embarrass the future.").

At the very least, this Court should affirm *Carpenter* as providing Fourth Amendment protection to extended periods of CSLI and defer to the Legislature to balance privacy concerns with law enforcement's use of limited periods of CSLI. But this Court did not grant certiorari to clarify *Carpenter*; hence, this Court should finalize CSLI precedent and set forth the fine-line distinction between *Carpenter* CSLI and more limited periods of CSLI. This Court should also apply its longstanding precedents, *Smith* and *Miller*, for third-party records that fall outside the "distinct category of information" obtained in *Carpenter* and *Jones*. *Id.* at 318.

If this Court determines that *Carpenter* should be the extent of the Judiciary's reach on policy considerations for law enforcement's use of CSLI, this Court should hold that *Carpenter* does not extend to Agent Hale's limited CSLI requests and allow Congress to evaluate bills that have been introduced to amend the SCA. *See* ECPA Modernization Act of 2017, S.B. 1657 (2018) (proposing to amend the SCA a require a warrant for both stored content and geolocation information stored by third-party service providers). The Legislature is equipped with an abundance of tools and resources to consider the privacy and security interests for CSLI records

obtained in criminal investigations. *United States v. Graham*, 824 F.3d 421, 439 (4th Cir. 2016) (en banc) (Wilkinson, J., concurring) ("Faced with a term literally crying out for balance between the competing interests of individual privacy and societal security, it is appropriate to accord some degree of deference to legislation weighing the utility of a particular investigative method against the degree of intrusion on individuals' privacy interests.").

If this Court believes it should finalize *Carpenter*, rather than defer to the Legislature, then this Court should supplement *Carpenter* with sufficient, yet distinctive, guidance for less than seven days' worth of CSLI lawfully obtained under the SCA. The restricted and particularized nature of Agent Hale's CSLI requests sets the stage for this Court to establish bright-line precedent distinguishing the categories of *Carpenter* CSLI and more limited periods of CSLI. Perhaps, by holding that Agent Hale's requests were necessarily limited to avoid infringing Fourth Amendment interests, this Court would establish its restraints on warrantless CSLI to 72 hours for continuous CSLI and 100 hours for CSLI during business hours not to exceed the span of two weeks. *See Cty. of Riverside v. McLaughlin*, 500 U.S. 44, 58 (1991) (setting the 48-hour rule for judicial probable cause determinations when holding that law enforcement acted reasonable when obtaining the determination within 48 hours). This rule would conform to this Court's reasoning in *Carpenter* because *Carpenter* expressly refused to address more limited periods of CSLI. 138 S. Ct. at 2219.

Additionally, *Carpenter* only declined to extend the *Smith* and *Miller* third-party doctrine to more than a week's worth of CSLI requests. *Id.* at 315; *Smith v. Maryland*, 442 U.S. 735, 742 (1979); *United States v. Miller*, 425 U.S. 435, 444 (1976). The *Carpenter* Court distinguished *Smith* and *Miller* because pen registers and bank statements, respectively, did not provide an "exhaustive chronicle of location information," unlike the *Jones* GPS tracking and the *Carpenter*

CSLI records. *Id.* at 318. Here, there is no "world of difference" between Agent Hale's limited, short-term CSLI requests and "the limited types of personal information addressed in *Smith* and *Miller*," like there was in both *Jones* and *Carpenter*. *Id.*

This Court, in *Smith* and *Miller*, held that individuals have no legitimate expectation of privacy in information voluntarily disclosed to third parties and in the sole possession and control of third parties. *Smith*, 442 U.S. at 742 (holding that that there was no reasonable expectation of privacy in numbers dialed because all "telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."); *Miller*, 425 U.S. at 444 (holding that a person depositing money at a bank had no reasonable expectation in the privacy of the bank's transaction records, including his credit card statements). Even if the records contain personal and sensitive information, the third-party doctrine permits the Government to compel production without a warrant. *Carpenter*, 138 S. Ct. at 2223 (Kennedy, J., dissenting). The Government can subpoena third-parties and obtain individuals' bank records, telephone records, and credit card statements without conducting a search under the Fourth Amendment. *Id.*

Smith and *Miller* should apply to the Three-day Records and the Weekday Records because Delos Wireless had sole possession and control over them and they were so limited that *Carpenter's* refusal to extend the third-party doctrine to CSLI carries little weight. (Affidavit). Moreover, the limited CSLI records here reveal no more intrusive information than the *Miller* bank records or the *Smith* phone calls. *See Carpenter*, 138 S. Ct. at 2224 (Kennedy, J., dissenting) ("Cell-site records are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process.").

The bank records disclosed in *Miller* provided location data and were obtained through a third-party, just like the *Carpenter* CSLI and the CSLI here. *See Miller*, 425 U.S. at 437. However, the *Carpenter* CSLI provided significantly more location points than both the *Miller* bank records and Agent Hale's CSLI requests. The Three-day Records and the Weekday Records were also more limited than the bank records in *Miller* and also revealed less sensitive information than an individual's credit card statement typically does. Thus, if this Court allows the Government to subpoena unlimited third-party bank records, then surely limited CSLI requests are governed by the appropriate compulsory standard under the SCA.

Similarly, the Government can compel pen register information and track every phone call someone makes inside their own home for however long. *See Smith*, 442 U.S. at 739. Because pen registers capture the phone calls from a landline, the law enforcement in *Smith* could tell when Smith was at home and essentially track his location where the highest expectation of privacy exists. Because those records are used in the regular conduct of the phone company's business, a fact of which individuals are aware of, this Court held that no reasonable expectation of privacy exists. *Id.* at 744.

The limited CSLI records here, like *Smith*, potentially gave law enforcement location information while the suspect was within private premises, which was at most *de minimis* and of no use to the investigation. Regardless, such information is not within an individual's "legitimate expectation of privacy" when voluntarily disclosed to a third-party. *Id.* at 742.

Similar to *Smith*, where placing calls voluntarily conveyed the phone numbers to the telephone company, cell phone users voluntarily share their location data when transacting with cell phone providers to use the capabilities of current smartphones. *See* Jennifer Valentino-DeVries, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y

TIMES (Dec. 10, 2018) ("Companies that use location data say that people agree to share their information in exchange for customized services, rewards and discounts."). The limited CSLI records and the *Smith* pen register information are also analogous because cell phone users generally know their smartphones track their locations like landline users generally knew their outgoing call information is kept by phone companies. *See id.*

The *Carpenter* majority still asserts that a cell phone's location data is not truly "shared" in the context of *Smith* and *Miller* when in fact it is quite to the contrary. 138 S. Ct. at 2220. Justice Kennedy rightly recognizes that the comparison between the decision to transact with banks because cell phones are as necessary as having credit cards today. *See id.* at 2233 (Kennedy, J., dissenting) ("And the decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone.").

This Court should extend *Smith* and *Miller* to the present action because there is no significant distinction between the information revealed from limited periods of CSLI and bank records or call logs. Even if *Smith* and *Miller* do not govern, Agent Hale's limited CSLI requests are beyond the scope of *Carpenter* and this Court can defer to the Legislature or provide an affirmative rule that permits law enforcement to continue to obtain limited CSLI requests, confined to certain lengths of time, through the SCA compulsory process.

C. *Carpenter* Should Not Apply to the Tower Dump Requests Because Tower Dumps Do Not Provide a Comprehensive Record of a Person's Movements.

Tower dumps do not provide the type of location monitoring that is protected after *Carpenter* because tower dumps merely identify the phone numbers that connected to a specific tower, usually in a very short window of time. (R. at 4). In *Carpenter*, this Court was more concerned about CSLI records that allow law enforcement to track an individual's movements over a substantial period of time. 138 S. Ct. at 2219. This Court did not express a view on tower

dumps in *Carpenter*, but it did provide a few motivations for affording Fourth Amendment protection to certain types of CSLI. *Id.* at 2220.

The unique nature of extended periods of CSLI was central to this Court's decision in *Carpenter*. *Id.* at 2219 (holding that an individual maintains a legitimate expectation of privacy in the extensive record of his physical movements captured through CSLI). In *Carpenter*, this Court illustrated CSLI as "track[ing] nearly exactly the movement of [a cell phone's] owner." *Id.* at 2218. This Court also defined a tower dump as "a download of information on all the devices that connected to a particular cell site during a particular interval." *Id.* at 2220.

Tower dumps are not subject to additional Fourth Amendment protection after *Carpenter* simply because *Carpenter* dealt with far more intrusive location information. Indeed, Carpenter's counsel also conceded at oral argument that tower dumps would be unaffected by the Court's decision. *See* Albert Gidari, *The Practical Impact of Carpenter v. United States*, STANFORD L. SCH.: CTR. FOR INTERNET & SOC'Y (Nov. 30, 2017, 4:36 PM). A list of phone numbers that used a tower at a particular time is remarkably different than CSLI records that provide an "exhaustive chronicle" of an individual's movements.

Lower courts have recognized various types of information that fall outside *Carpenter* that do not reveal the kind of minutely detailed log of "the whole of [a person's] physical movements" that concerned the *Carpenter* Court. 128 S. Ct. at 2221; *United States v. Monroe*, No. CR 16-00055 WES, 2018 WL 5717367, at *5 (D.R.I. Nov. 1, 2018) (holding that *Carpenter* did not require the Government to obtain a warrant to compel disclosure of a unique IP address for any device that had downloaded the illicit files); *United States v. Evans*, No. 5:17-CR-39-FL-1, 2018 WL 7051095, at *2 (E.D.N.C. Dec. 20, 2018) (ruling that Carpenter does not apply to a warrant for substantive data, such as call logs and text message content, as opposed to location

data); *United States v. Kubasiak*, No. 18-CR-120-PP, 2018 WL 4846761, at *6 (E.D. Wis. Oct. 5, 2018) (holding that a surveillance camera fixed at the defendant's backyard was not a search under *Carpenter* because the camera could only observe the defendant in one location and could not track him around the neighborhood).

Here, Agent Hale's request for three tower dumps from the cell site near the three Sweetwater ATMs amounted to just an hour of cell-tower data from each of the three towers. (R. at 4). If *Carpenter* affirms the *Riley* and *Smith* conclusions that telephone call logs do not amount to searches, then three hours of cell number production is not a search. *Carpenter*, 138 S. Ct. at 2219 ("as explained in Riley, telephone call logs reveal little in the way of 'identifying information.'"). Three hours of cell phone numbers certainly does not provide the type of "pervasive tracking" that *Carpenter* was concerned about. *Id.* at 2220.

This information strictly limited Agent Hale to determine Appellant's location at one specific time. Ultimately, this Court in *Carpenter* explicitly distinguishes this type of information from the location information protected by the Fourth Amendment. *Id.* ("Yet this case is not about 'using a phone' or a person's movement at a particular time.").

This Court should hold that, after *Carpenter*, CSLI records from tower dumps do not constitute a search under the Fourth Amendment. Therefore, Agent Hale properly obtained each of the three CSLI records through the lawful, compulsory process under the SCA.

CONCLUSION

For the foregoing reasons, Respondent respectfully requests this court to affirm the holding of the Fourteenth Circuit, and deny Appellant's motion to suppress evidence.

Respectfully Submitted,

Attorneys for Respondent