DOCKET NO. 10-1011

IN THE

Supreme Court of The United States

HECTOR ESCATON,

PETITIONER,

v.

UNITED STATES OF AMERICA.

RESPONDENT.

ON WRIT OF CERTIORARI FROM THE UNITED STATES COURT OF APPEALS,
FOURTEENTH CIRCUIT

BRIEF FOR RESPONDENTS

COUNSEL FOR RESPONDENTS

February 10, 2019

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES iii

QUESTIONS PRESENTED v

OPINION BELOW v

CONSTITUTIONAL PROVISIONS AND RULES v

INTRODUCTION 1

STATEMENT OF THE CASE 3

ARGUMENT 6

I. **BORDER SEARCHES ARE A LONG STANDING EXCEPTION TO THE FOURTH AMENDMENT'S WARRANT REQUIREMENT, THEREFORE, DO NOT REQUIRE REASONABLE SUSPICION** 6

A. Riley Did Not Disturb the Border Search Exception. 8

B. Border Searches of Electronic Devices Do Not Require Reasonable Suspicion. 9

C. Even If the Distinction Between Routine and Nonroutine Border Searches Require Differing Levels of Suspicion, the Search That Occurred Was Routine and Therefore Did Not Need Reasonable Suspicion. 10

II. **THE STORED COMMUNICATIONS ACT** 12

III. **THE *CARPENTER* DECISION** 13

IV. **POST-*CARPENTER* DEVELOPMENTS** 14

V. **TWO HISTORICAL CSI COURT ORDERS FOR LESS THAN SEVEN DAYS DO NOT VIOLATE THE FOURTH AMENDMENT IN LIGHT OF THE HOLDING IN *CARPENTER* WHEN THEY WERE REASONABLY NARROW REQUESTS AND ALSO DID NOT VIOLATE THE CSA**. 15

A. The "Three-Day" Request Was Substantially Less Than the Seven-Day Limit Imposed in *Carpenter*, and Was Reasonably Limited to the Time Frame During Which the ATMs Were Infected With Malware 16

B. The "Weekday Records" Request Only Amounted to 100 Hours of Information, Significantly Less Than the 168 Hour Limited Imposed Under *Carpenter*, and Was Reasonably Limited to the Times During Which the ATMs Were Accessible 18

VI. **ONE HOUR OF CELL TOWER INFORMATION REQUESTED VIA COURT ORDER DOES NOT VIOLATE THE FOURTH AMENDMENT OR THE SCA, AND DOES NOT TRIGGER THE "TRACKING" CONERNS CONTEMPLATED IN *CARPENTER* THAT HISTORICAL CSLI INFORMATION TRIGGERS** 20

CONCLUSION 21

SIGNATURE BLOCK 21

TABLE OF AUTHORITIES

CASES PAGE

Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523 (1987) 21

In the Matter of the Application of the United States of American for an Order Pursuant to 18 U.S.C. 2703(d), (W.D. Tex. Nov. 10, 2019).....16

Kyllo v. United States, 533 U.S. 27 (2001).....19

Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018)..20

Riley v. California, 573 U.S. 2473 (2014).....7, 8, 11

Schneckloth v. Bustamonte, 412 U.S. 218 (1973) 6

United States v. Chavez, 894 F.2d 593 (4th Cir. 2018) 14, 17

United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013).....3, 9, 10, 11

United States v. Curtis, 901 F.3d 846 (7th Cir. 2018).....14, 17

United States v. Dalia, 441 U.S. 238 (1979) 12

United States v. Dattmore, No. 12-Cr-166A, 2013 U.S. Dist. LEXIS 126342 (W.D.N.Y. Sept. 3, 2013).....11

United States v. Evans, 2018 US. Dist. LEXIS 219506 (E.D.N.C. Dec. 20, 2018) 12, 13

United States v. Farrad, 895 F.3d 859 (6th Cir. 2018).....14, 17

United States v. Flores-Montano, 541 U.S. 149 (2004) 7, 9, 10

United States v. Hargett, No. 5:15-CR-374-D (E.D.N.C. Aug. 17, 2018) 13

United States v. Jones, 565 U.S. 400 (2012) 15, 16, 19, 20

United States v. Joyner, 899 F.3d 1199 (11th Cir. 2018) 14, 17

United States v. Knotts, 460 U.S. 276 (1983) 18, 19

United States v. Kolsuz, 890 F.3d 133 (4th Cir. 2018) 10, 11

United States v. Miller, 425 U.S. 435 (1976).....14, 15

United States v. Montoya de Hernandez, 473 U.S. 531 (1985).....7

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

United States v. Myles, No. 5:15-CR-172-F-2, U.S. Dist. LEXIS 55326 (E.D.N.C. Apr. 26, 2018) 13

United States v. Ramsey, 431 U.S. 606 (1977).....6, 7, 8

United States v. Streett, 2018 U.S. Dist. LEXIS 201025 (D.N.M. Nov. 27, 2018).....15

United States v. Touset, 890 F.3d 1227 (2018).....9

United States v. Zodhiates, 901 F.3d 137 (2d Cir. 2018).....14, 17

CONSTITUTIONAL PROVISIONS PAGE

U.S. CONST. AMEND IV .....v, 6

STATUTES PAGE

18 U.S.C. § 2703(a) ..... vi, 5, 12

QUESTIONS PRESENTED

I. Does the Fourth Amendment border search exception have a special carve out for electronic devices even if the search that occurred at the border could be correctly categorized as a routine search?

II. May the government request historical CSLI and cell tower dumps via court order for less than seven days per the holding in *Carpenter* and the text of the SCA for a reasonably limited period of time?

OPINION BELOW

The United States District Court of West Texas ("District Court") denied a motion to suppress evidence resulting from a forensic search and a cell-site data request. The District Court rejected the invitation to exempt electronic devices from the Fourth Amendment's border search exemption. The United States Court of Appeals for the Fourteenth Circuit ("Fourteenth Circuit") affirmed the District Court's denial of the motion to suppress because the border search did not require any reasonable suspicion before conducting a forensic examination of the electronic devices and found that the cell site data requested complied with the requirements set forth in *United States v. Carpenter*. 138 S. Ct. 2206 (2018).

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment to the United States Constitution, U.S. Const. amend IV, 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."

The Stored Communications Act, 18 U.S.C. § 2703(a), provides:

> "A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eight days. . ."

INTRODUCTION

Respondent, United States of America, in the matter of *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021), before the United States Court of Appeals, Fourteenth Circuit, respectfully submit this brief on the merits and urge the Court to affirm the Fourteenth Circuit's decision below.

Summary of the Argument

This case concerns the ability of the government to protect citizens within the confines of the Fourth Amendment and the Stored Communications Act. This Court should affirm the Fourteenth Circuit's decision below, because the government did not violate the standards set forth by Carpenter, or otherwise violate Hector Escaton's Fourth Amendment rights, either via the border search of his devices without assistive technology, nor via the CSLI or cell tower dump data obtained via court order.

The Supreme Court has never required reasonable suspicion in respect to the border search exception. Consequently, the search of defendant's electronic devices was lawfully conducted by Officer Stubbs and Officer Cullen despite lacking reasonable suspicion. Moreover, there is no basis to require reasonable suspicion for routine or nonroutine border searches of property as the Court has never recognized this distinction in relation to the border search exception. However, even if, the distinction between routine and nonroutine is found to be relevant, the search presented in this case was squarely within a routine border search and therefore did not require reasonable suspicion.

The court orders for historical CSLI information for Escaton for the "Three-Day records" and the "Weekday records" were requested pursuant to the SCA under § 2703(d), and did not

overstep the boundaries laid out by *Carpenter*. The Court limited the ability for the government to obtain historical CSLI without a warrant issued upon probable cause for periods of seven days (168 hours) or greater. Here, both orders were for periods substantially shorter than that amount: for three full consecutive days, and for the business hours of 8:00 AM to 6:00 PM for ten weekdays, respectively. Neither the Court nor the SCA have affirmatively prohibited such requests when made by a court order. Therefore, the government requests for the historical CSLI did not violate Escaton's Fourth Amendment rights. Even if the CSLI requests are found to be a derivation from the Court's intention in *Carpenter*, the government's requests were made in good faith under the legal framework at the time, and should be upheld.

Additionally, the government's request for three cell tower dumps for a total of one hour's worth of information did not violate Escaton's protections under the Fourth Amendment, or run contrary to the SCA. The type of information provided to the government by the cell service providers are less intrusive than the information that may be obtained via historical CSLI. Moreover, this extremely limited time frame and geographical area outlined in the request limited the amount of innocent third-parties' private information that could be shared. It was also as reasonably narrow as possible to attempt to locate the suspicious individual who interacted with the attacked ATMs in question. The 30-minute window both before and after the individual approached the machines would also not be able to provide sufficient information to authorities that would constitute the type of tracking the Court is wary of in cases of GPS or dragnet surveillance.

For the reasons outlined below, the United States of America requests that the Court affirm the decision of the Fourteenth Circuit.

Standard of Review

This questions on appeal contain mixed questions of fact and law, and thus must be reviewed under the de novo standard and for clear error, respectively. *See 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)).

STATEMENT OF THE CASE

Statement of Facts

Hector Escaton (hereinafter referred to as "Escaton") was involved in an illegal skimming operation with Delores Abernathy (hereinafter referred to as "Abernathy") during the month of October 2018. *See* R. at 3. This scheme took place in two neighboring cities Escalante and Sweetwater, of West Texas. *See id.* Seven total Automated Teller Machines (ATMs) were targeted in the densely populated city of Sweetwater, and less urban city of Escalante via (1) injection of malware via the USB port, (2) physical skimmers overlaying debit card readers, accompanied by small cameras that obtained PINs, and (3) via a sophisticated malware system allowing the schemers to withdraw cash from the machine. *See id.* at 3-4; Hale Aff. #11.

This criminal scheme resulted in hundreds of Mariposa Bank customers' identities being stolen, and false accounts being created without their knowledge or consent. *See id.* at 4. These customers were also personally injured by the criminals' direct withdrawals on their accounts. *See id.* The total estimated losses amount to $50,000 during the month of October 2018. *See id.*

Escaton, a 28-year-old part-time bartender, was returning to West Texas from Mexico through a border checkpoint on West Texas. *See id.* at 2; Hale Aff. #8. During his passage, U.S. Customs and Border Patrol (CBP) Agent Ashley Stubbs conducted a routine border inspection of Escaton's vehicle. *See id.* This search revealed the presence of three large suitcases, an iPhone,

laptop, three external hard drives, and four USB devices. *See id.* Agent Stubbs conducted manual search of the devices without the use of assistive technology, a wireless connection, or passwords. *See id.* A note was identified near the keyboard of the laptop which stated "Call Dolores (201) 181-0981 $$$." *See id.* The laptop contained password protected files, and the USB contents were not readily visible when connected to the computer *See id.* at 2-3. Officials later connected Abernathy to Escaton, and the rest of the scheme. *See id.* at 5. She was previously convicted for ATM skimming. *See id.*

Agent Stubbs contacted Immigrations and Customs Enforcement (ICE) Senior Special Agent (SSA) Theresa Cullen, also a Computer Forensic Examiner, to conduct a process by which she would copy and scan the devices. *See id.* at 3. SSA Cullen, upon reviewing these devices, located the confidential banking information and pins for various individuals. *See id.* The USB devices also revealed traces of malware that were similar, although not exactly identical to the kind used at the Sweetwater Mariposa ATMs. *See id.* at 3, 5. SSA Cullen promptly deleted the other non-incriminating scans. *See id.* Based upon these findings, the CBP informed the Federal Bureau of Investigation (FBI) of the findings, which they believed related to the Mariposa Bank ATM skimming case. *See id.*

Evidence of this illicit skimming scheme was first brought to light on October 13, 2018, when Maeve Millay, the local branch manager for the Boswell Street Mariposa Bank branch, discovered tampering of one of the ATMs. *See id.* at 3. The ATM in question was serviced two days prior on October 11, 2018. *See id.* at 5. Surveillance photos near the ATMs saved images of a suspicious looking man in a black sweatshirt, who approached the ATMs. *See id.* at 4.

Agent Hale of the FBI was responsible for investigating this matter. *See id.* She coordinated with U.S. Attorney Elsie Hughes to request three tower dumps from cell sites in

close proximity to the affected Sweetwater ATMs, for 30 minutes before and after the suspect approached the ATMs, in a matter consistent with the Stored Communications Act (SCA) 18 U.S.C. § 2703(d). *See id.* She also obtained court orders under the same statute to acquire the historical CSLI of Escaton, via his provider, Delos Wireless, for the period of October 11th through October 13th (hereinafter "Three-Day Records"), during which the ATMs were vandalized. *See id.* at 5. The other request for Escaton and Abernathy's historical CSLI encompassed the weekday work hours of October 1st through October 12th. *See id.* This request only covered the hours of 8:00 AM MDT through 6:00 PM MDT, which were the only times that the ATMS, located inside the bank, were accessible. *See id.*; Hale Aff. #17.

Although Escaton was not found to be in the Escalante area from October 11-13th, he was placed in the area of the Sweetwater Boswell Branch ATM on October 12th. *See* R. at 5. His phone number was revealed as pinging from a cell tower near the attacked ATMs according to the information yielded by the one-hour cell tower dump. See Hale Aff. #19. The malware on his USBs was similar to that of the malware used Sweetwater Mariposa ATMs. *See* R. at 5. Following the routine border search, cell tower, and historical CSLI information data gathering process, Escaton was charged with and subsequently convicted of 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. *See* R. at 2. Escaton's motion to suppress the forensic border search and CSLI request evidence was denied by the district court, and affirmed on appeal at the Fourteenth Circuit. This appeal followed. *See id.*

Procedural History

The government indicted defendant Escaton for Bank Fraud, Conspiracy to Commit Bank Fraud, and Aggravated Identity Theft after conducting a forensic search of his electronic devices

during a routine border search. 18 U.S.C. § 1344; 18 U.S.C. § 1349; 18 U.S. § 1028A; R. at 6. The evidence that resulted in his indictment was obtained during a forensic search of his electronic devices and a subsequent cell-site data request from Delos Wireless. Defendant sought to suppress the evidence originally gathered during the forensic search in violation of his Fourth Amendment right because the officers conducted the search with no reasonable suspicion. As to the suppression of cell-site data evidence, defendant argued that the three sets of data collection did not comply with *Carpenter* and therefore were illegal. The District Court denied the motion to suppress the evidence obtained during the forensic search and cell-site data requests. R. at 11. The Fourteenth Circuit affirmed. This appeal followed.

ARGUMENT

I. BORDER SEARCHES ARE A LONG STANDING EXCEPTION TO THE FOURTH AMENDMENT'S WARRANT REQUIREMENT, THEREFORE, DO NOT REQUIRE REASONABLE SUSPICION.

The United States Constitution provides: "the right of the people to be secure in their persons, houses, papers, papers, and effects, against unreasonable searches and seizures." U.S. Const. Amend. IV. The Fourth Amendment guarantees freedom from unreasonable searches and seizures. *See Schneckloth v. Bustamonte*, 412 U.S. 218, 222 (1973). However, searches that occur at the border are different. *See United States v. Ramsey*, 431 U.S. 606, 619-20 (1977). There is a heightened national security interest in preventing illegal activity from entering the country. As such, border searches do not require the full panoply of Fourth Amendment protections – government agents may conduct routine searches and seizures of property without a warrant or reasonable suspicion. *United States v. Ramsey*, 431 U.S. 606, 619-20 (1977).

The primary reason for a border search is to protect against from unwanted and illegal activity from entering the country. As such, the Supreme Court created the border search exception which is "grounded in the recognized right of the sovereign to control, subject to

substantive limitations imposed by the Constitution, who and what may enter the country." *United States v. Ramsey*, 431 U.S. 606, 620 (1977). Searches at the border therefore do not require the full unmitigated protection of the Fourth Amendment so that the government may protect national security.

Moreover, border searches are inherently reasonable under the Fourth Amendment and therefore do not typically require reasonable suspicion. Simply put, international travelers are not in their home; they are at the port of entry to the United States. Their expectation of privacy is substantially lessened. As such, the Supreme Court has only once required reasonable suspicion for a border search which involved a prolonged detention and a search of her alimentary canal - a literal, physical invasion of her person. *United States v. Montoya de Hernandez*, 473 U.S. 531, 541-44 (1985). Outside of this specific case, the Supreme Court has rejected a hard a fast rule for what level of suspicion is necessary to conduct border searches, if any. *United States v. Montoya de Hernandez*, 473 U.S. 531, 542 n. 4 (1985) ("It is important to note what we do not hold. Because the issues are not presented today we suggest no view on what level suspicion, *if any*, is required for non-routine border searches."); *United States v. Flores-Montano*, 541 U.S. 149, 152 ("[t]he reasons that might support a requirement of some level of suspicion in the case of highly intrusive searches of the person-dignity and privacy interests of the person being searched . . . have no place in border searches of vehicles.").

Despite this pronouncement, some courts have created a new rule to the border search exception as it relates to forensic searches of electronic devices. Courts have done this for two primary reasons: (1) confusion regarding the *Riley* decision as it applies to border searches and as a result (2) have created a distinction between routine and non-routine searches.

A. Riley Did Not Disturb the Border Search Exception

The border search exception has been left untouched by the narrow holding in *Riley v. California*. In *Riley v. California*, the Supreme Court held that Fourth Amendment warrant requirement still applied to the search of digital data even when that search occurred incident to arrest. 134 S. Ct. at 2485. The search that occurred in *Riley* did not occur at an international port of entry as the search conducted by Officer Stubbs and Cullen. *See id.* Instead, the search in *Riley* occurred a result of a traffic stop within the national borders. Consequently, Riley was afforded the full panoply of Fourth Amendment protection; searching Riley's electronic devices furthered no legitimate national security interest. Here, however, the search of defendant's electronic devices further secured the border and helped to detect ongoing illicit activity.

Moreover, the Court in *Riley* merely asked whether "the application of the search incident to arrest doctrine [to searches of digital data] . . . would untether the rule from the justifications" for the specific exception at issue. 134 S. Ct. at 2485. In *Riley*, the specific exception to the Fourth Amendment's warrant requirement was incident to arrest. *Id.* Ultimately, the Court decided that searching defendant's cell phone, did in fact, untether it from the purposes of creating the exception in the first place: to protect officers from *physical* threats. *Id.* Here, however, that is not the case. The border search exceptions to the Fourth Amendment have always been justified "pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country" to protect against illegal activity from crossing our borders at jeopardizing national security. *United States v. Ramsey*, 431 U.S. at 616.

Consequently, *Riley* has no application to border searches like the one conducted by Officer Stubbs and Officer Cullen. Allowing officials to conduct a forensic search of their

electronic devices certainly does no offend the underlying justifications to the border search exceptions. If anything, allowing the search only bolsters the purpose and proves why they are necessary to effectively secure the border from illegal activity like the fraud at issue here.

B. Border Searches of Electronic Devices Do Not Require a Higher Level of Suspicion

The Supreme Court has never required reasonable suspicion to a border search of property. *See United States v. Flores-Montano*, 541 U.S. 149 (2004). Moreover, the Court has declared that "[r]outine searches of the persons and effects of entrants" at the border are reasonable. *United States v. Montaya de Hernandez*, 473 U.S. 531, 538 (1985). It is also has never imposed that requirement on border searches of property despite the degree of intrusiveness. *See United States v. Touset*, 890 F.3d 1227, 1233 (2018). Importantly, the Court has never distinguished between different types of property either. *United States v. Cotterman*, 709 F.3d 952, 975 (Callahan, J. concurring in part, dissenting in part, and concurring in judgment).

As identified in *Touset*, the Court has also "rejected a judicial attempt to distinguish between 'routine' and 'nonroutine' searches and to craft "[c]omplex balancing tests to determine what constitutes a 'routine' search of a vehicle, as opposed to a more 'intrusive' search of a person." *United States v. Touset*, 890 F.3d 1227, 1233 (2018). Therefore, any distinction between a routine and non-routine border search is irrelevant as to whether a border search requires reasonable suspicion. The distinction becomes even less relevant when trying to create an exception for forensic searches that lawfully occur at the border.

The only distinction that makes a difference is the search of a person's body which is highly intrusive and particularly offensive. However, searching defendant's electronic devices, here, does not present that issue.

C. Even if the distinction between routine and non-routine search requires differing levels of suspicion, the search that occurred was routine and therefore did not need reasonable suspicion.

Although the Supreme Court has not ever based a decision on the distinction between routine and non-routine border searches, some sister circuits have created an altogether new category of what qualifies as routine or nonroutine border search. *See United States v. Kolsuz*, 890 F.3d 133 (4th Cir. 2018); *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc). In *Flores-Montano*, the Court rejected the invitation provided by the Court of Appeals to create a new balancing test to provide a distinction between what qualifies as a routine search and what might qualify as a less routine, and therefore, more intrusive. *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004).

According to the Fourth and Ninth Circuit, however, a routine border search never requires any reasonable suspicion, but a nonroutine border search requires reasonable suspicion. Under this view, the high degree of intrusion or perhaps the "particularly offensive manner" in which a nonroutine border search has been conducted requires the reasonable suspicion. *United States v. Kolsuz*, 890 F.3d 133, 143-44 (2018). To be clear, even the Fourth Circuit recognizes that "the Court has not delineated precisely what makes a search nonroutine . . . but as the district court explains, in deciding whether a search rises to the level of nonroutine, courts have focused primarily on how deeply it intrudes a person's privacy." *United States v. Kolsuz*, 890 F.3d 133, 144 (2018). Nevertheless, the court still creates the distinction between a routine and nonroutine border search despite a clear indication from Congress or the Supreme Court that there is a clear distinction.

Moreover, under this theory, courts have suggested that there is a distinction between a cursory and forensic search of electronics despite a clear legal basis for doing so. *See United*

States v. Cotterman, 709 F.3d 952, 978 (2018) (Callahan J., concurring) ("Even if the majority means to require reasonable suspicion for any type of digital forensic border search, no court has ever erected so categorical a rule, based on so general a type of search or category of property, and the Supreme Court has rightly slapped down anything remotely similar.") In a forensic search, a government agent can search the entirety of a computer's hard drive, including any files that might be password protected or any files that may have been intentionally deleted. *Id.* at 962-63 n. 9. Forensic searches allow the government official to recover and access more information than would be generally accessible on the computer. *See id.* As such, the Fourth and Ninth Circuits have held that these forensic searches of digital devices are nonroutine. These decisions are rooted in the idea that forensic searches of digital devices are intrusive because of the sheer quantity of accessible information and the sensitivity of that information. *United States v. Kolsuz*, 890 F.3d 133, 144 (2018). These courts have relied on *Riley* to create this distinction.

For the reasons stated above, the searches of electronic devices do not warrant a new rule for the border search exception. However, if there is a distinction between routine and nonroutine, then forensic searches of electronic devices like the search that occurred of defendant's items are routine. *See United States v. Dattmore*, No. 12-Cr-166A, 2013 U.S. Dist. LEXIS 126342, at *4 (W.D.N.Y. Sept. 3, 2013) (relying on past case law to conclude that "searches of computer and electronic devices are likewise considered routine searches that may be conducted in the absence of reasonable suspicion.") The fact that electronic devices are able to store more information than what would be carried in luggage is irrelevant as to whether it makes the search routine or nonroutine.

II. THE STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA) permits government officials to compel disclosure of certain electronic communications that is in electronic storage for up to one-hundred eighty days. *See* 18 U.S.C. § 2703(a). The government must either obtain a valid search warrant issued upon probable cause or provide a court order that 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought are relevant and material to an ongoing criminal investigation," to gain access to the stored communications information. *Carpenter*, 138 S. Ct. at 2212 (quoting 18 U.S.C. § 2703(d)).

The reasonable suspicion standard required for officials to obtain a court order under the SCA falls short of the probable cause requirement for a search warrant. *See id.* at 2221. Under *Carpenter*, the Court held that under the current SCA-Fourth Amendment framework, a court order is not sufficient to obtain historical CSLI for a consecutive seven-day period or more. *Carpenter*, 138 S. Ct. at 2212 (declining to decide whether collection of fewer than seven days worth of CSLI data without a warrant would violate the Fourteenth Amendment, even when the actual data collected only amounted to two days of information).

In order to have a valid search warrant, three basic requirements must be met: (1) the warrant must be signed by a neutral and detached judge or magistrate, (2) the warrant must be supported by probable cause, and (3) it must describe the places to be searched and things to be seized with particularity. *See United States v. Dalia*, 441 U.S. 238, 255 (1979). It is possible for the government to successfully assert that the underlying facts alleged to obtain a court order meet the requirement for a search warrant. *See id.*; *United States v. Evans*, 2018 U.S. Dist. LEXIS 219506 at *7 (E.D.N.C. Dec. 20, 2018) (holding that a court order for 60 days of historical CSLI that facially met the three requirements for a valid search warrant and met the

probable cause standard did not violate the defendant's Fourth Amendment rights). The fact that a court order is made under the SCA does not affect this analysis, so long as the requirements are otherwise satisfied. *See, e.g., Evans*, 2018 U.S. Dist. LEXIS 21506 at *11; United States v. Hargett, No. 5:15-CR-374-D (E.D.N.C. Aug. 17, 2018); United States v. Myles, No. 5:15-CR-172-F-2, 2016 U.S. Dist. LEXIS 55326 at *7-8 (E.D.N.C. Apr. 26, 2018).

III. THE *CARPENTER* DECISION

The Court in *Carpenter* held that the government's acquisition of defendant's historical cell-site location information (CSLI) constituted a search under the Fourth Amendment. *See Carpenter*, 138 S. Ct. at 2206-08. CLSI is comprised of time-stamped records made by individuals each time their phones connect to radio antennas, otherwise known as "cell sites." *Id.* at 2208. This information can be used to develop a comprehensive history of where an individual was located at different points in time. *See id.* The precision of CSLI records is affected by various factors, including population density, coverage area, and the number of cell towers in the given area. *See Carpenter*, 138 S. Ct. at 2211-12.

The majority found that this search violated defendant's reasonable expectation of privacy when the court order used to obtain the information did not demonstrate probable cause, and when one of the orders yielded defendant's CSLI information for longer than a consecutive seven-day period. *See id.* at 2212 (finding that CSLI collected for a four-month period and then a seven-day period violated defendant's reasonable expectation of privacy when there was no probable cause provided for a warrant).

The Court carefully distinguished though that although technically only two days' worth of CSLI data was in-fact produced by the cell service provider in this case, that they were only narrowly holding the seven-day record request as a search requiring a warrant. *See id.* at 2217, n.

3. The Court explicitly declined to rule on cases where less than seven-days' worth of CSLI was requested, real-time CSLI collection, or "tower dumps." *See id.* at 2220. CSLI was noted by the Chief Justice Roberts as a technological advancement that "does not fit neatly under existing precedents." *See id.* at 2209.

IV. POST-*CARPENTER* DEVELOPMENTS

A. The Good Faith Exception

The *Carpenter* decision prompted a wave of appeals throughout the country through which convicted individuals challenged the constitutional basis of CSLI obtained against them under the SCA without a search warrant. The Second, Fourth, Sixth, Seventh, and Eleventh circuits have all held that so long as the government collected the CSLI in question in a manner that falls within the good faith exception to the exclusionary evidence rule, it would be upheld. *See, e.g.*, *United States v. Curtis*, 901 F.3d 846, 849-51 (7th Cir. 2018); *United States v. Joyner*, 899 F.3d 1199, 1205 (11th Cir. 2018); *United States v. Zodhiates*, 901 F.3d 137, 143 (2d Cir. 2018); *United States v. Chavez*, 894 F.2d 593, 608 (4th Cir. 2018); *United States v. Farrad*, 895 F.3d 859, 891 (6th Cir. 2018). The good-faith exception does not apply to CSLI evidence collected following the *Carpenter* decision, to the extent that it runs contrary to the Court's holdings. *See Carpenter*, 138 S. Ct. at 2221.

B. The Third-Party Doctrine

The third-party doctrine typically enables government officials to obtain business records, even when they contain personal or sensitive information. *See United States v. Miller*, 425 U.S. 435, 444 (1976); *Smith*, 442 U.S. at 744 By requesting such information from businesses for which individuals do not have a legitimate Fourth Amendment interest, the

government does not run afoul of Fourth Amendment protections. *See Miller*, 425 U.S. at 444; *Smith*, 442 U.S. at 744.

In *Carpenter*, the Court declined to extend the third-party doctrine exception to cases involving historical CSLI, due to the "unique nature" of these records. *See* 138 S. Ct. at 2209, 2220 (finding that individuals do not meaningfully release their information to cell service providers, and that mere collection by a third-party does not in itself preclude a Fourth Amendment claim). Historical CSLI was distinguished from business records for which one would ordinarily have a reduced expectation of privacy. *See id.* at 513-14. CSLI has been deemed analogous to GPS records, which do not always require a warrant, but for which the Court has agreed that prolonged periods of monitoring may arise to the level of a search under the Fourth Amendment. *See Jones*, 565 U.S. at 430.

The holding in *Carpenter* was intentionally crafted narrowly enough so as not to touch "other business records that might incidentally reveal location information." *Id.* However, the telephone numbers one dials continue to fall under the third party exception, and may be sought without a warrant. *See Streett*, 2018 U.S. Dist. LEXIS 201025 at *20 (citing *Carpenter*, 138 S. Ct. at 2209).

V. TWO HISTORICAL CSI COURT ORDERS FOR LESS THAN SEVEN DAYS DO NOT VIOLATE THE FOURTH AMENDMENT IN LIGHT OF THE HOLDING IN *CARPENTER* WHEN THEY WERE REASONABLY NARROW REQUESTS AND ALSO DID NOT VIOLATE THE CSA

At this time, the *Carpenter* decision narrowly held that collection of more than 168 hours or seven days of historical CSLI without a warrant issued upon a showing of probable cause. *See Carpenter*, 138 S. Ct. at 2221. However, the Court explicitly declined to rule on such collection of information for less than seven days, even though the cell service provider only gave two days' worth of information. *See id*. at 2212. This suggests that the Court intended to limit the

analysis to seven days or 168 hours' worth of data, and not rule on the constitutionality of fewer days' worth of data without a warrant.

The precision of CSLI records is affected by various factors, including population density, coverage area, and the number of cell towers in the given area. *See Carpenter*, 138 S. Ct. at 2211-12. The main concern expressed by the Court relates to the ability to retroactively track every movement of a subject, similar to GPS monitoring outlined in *Jones*. *See id.* at 2210 (citing Jones, 565 U.S. at 412. The substantially limited nature of the government's investigative efforts were designed to minimize collection of innocent third-party information, identify the parties involved in the financial fraud scheme, and protect the community from further compromise of confidential data. *See* R. at 2-5.

In this case, both of the CSLI requests were made by FBI agents via court orders, rather than search warrants. *See* Hale Aff. Agents provided sufficient information to demonstrate that there were "specific and articulable facts showing that there [were] reasonable grounds to believe that the records and other information sought [were] relevant and material to [the] ongoing criminal investigation." *In the Matter of the Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d)* (W.D. Tex. Nov. 10, 2019).

A. The "Three-Day" Request Was Substantially Less Than the Seven-Day Limit Imposed in *Carpenter*, and Was Reasonably Limited to the Time Frame During Which the ATMs Were Infected with Malware

The first CSLI request was for a three-day span, from October 11th through October 13th, 2018. *See* R. at 5. The records were specifically requested for Escaton's phone only. *See id*. This period of time specifically related to the time between the ATM's previous maintenance inspections, when the vandalism was identified. *See* Hale Aff. #17.

Escaton was identified as being in the vicinity of the Sweetwater Boswell Branch ATM on October 12th. See R. at 5. Sweetwater cell towers collect cell-site data approximately every five-to-ten minutes, and may provide data concerning the location of the target phone as accurately as within 50 feet of the phone. *See* Hale Aff. #11. There are many physical structures in this urban area, and therefore some buildings have additional cell towers to improve cell service for subscribers. *See id.* It is true that on occasion, the CSLI collected through this technique may be more accurate than GPS data. *See id.*

However, the request made in this situation still falls significantly short of the seven-day limitation set forth in *Carpenter*, and does not raise privacy concerns that the search was unreasonable in response to the scope or length of the request. *See* 138 S. Ct. at 2221. The request was reasonably limited to the minimum length of time necessary to establish whether Escaton's phone was in the vicinity of the Escalante ATMs during the three-day window when it was vandalized and infected with malware. *See* Hale Aff. #17. Moreover, the only data requested was that of Escaton, not other innocent third-parties. *See id.* at 5. Therefore, the concerns regarding the collection of third-party data are inapplicable.

Even if the request of three consecutive days' worth of CSLI without a warrant would ultimately be considered by the Court as an impermissible extension of the holding in *Carpenter*, the CSLI collection should be held as acceptable per the good faith doctrine. *See, e.g.*, *United States v. Curtis*, 901 F.3d 846, 849-51 (7th Cir. 2018); *United States v. Joyner*, 899 F.3d 1199, 1205 (11th Cir. 2018); *United States v. Zodhiates*, 901 F.3d 137, 143 (2d Cir. 2018); *United States v. Chavez*, 894 F.2d 593, 608 (4th Cir. 2018); *United States v. Farrad*, 895 F.3d 859, 891 (6th Cir. 2018). The government officials' reasonable request, taken in good faith, with the intent to minimize government interference as to the CSLI collection, demonstrates a good faith

intention to operate within the confines of the *Carpenter* holding and the Stored Communications Act. *See, e.g.*, *Carpenter*, 138 S. Ct. at 2221.

Therefore, the Court should affirm the lower court's decision as to the legality of the three-day records.

B. The "Weekday Records" Request Only Amounted to 100 Hours of Information, Significantly Less Than the 168 Hour Limited Imposed Under *Carpenter*, and Was Reasonably Limited to the Times During Which the ATMs Were Accessible

The second CSLI request applied to both Escaton's and Abernathy's phone numbers for the hours of 8:00 AM until 6:00 PM during the weekdays spanning October 1st through October 12th, 2018, and Abernathy's subscriber information. *See* R. at 5. This time period encompassed the time period of the ATM skimming activities, up until the financial fraud activities were uncovered on October 13th. *See id.* at 3. The collection of Abernathy's CSLI information or subscriber information are not at issue in this case.

The limited nature of this request only encompassed weekday work hours for the average individual, and the only hours during which the banks' ATMs were operational and accessible. *See* Hale Aff. #17. Additionally, the request was made for 100 hours of data, which falls short of the limitation set forth by the Court in in *Carpenter* by forty percent. *See Carpenter*, 138 S. Ct. at 2221; R. at 5 n.7. Moreover, the request was not comparable to the 24-hour around-the-clock nature as contemplated in *Knotts*. *See* 460 U.S. at 281. This demonstrates the government's clear concern to not overstep the limitations set forth by the Constitution or the Court, and their attempts to consciously limit the scope of this CSLI data collection effort.

While Petitioner may contend that the temporal period of records requested extended beyond the seven consecutive days allowed in *Carpenter*, the Court took into account the total hours of the request when determining the constitutionality of the request. *See Carpenter*, 138 S.

Ct. at 2212. Here, the 100 total hours requested over the span of ten business weekdays did not exceed the number of hours that presumptively required a warrant per *Carpenter*. *See id.*; R. at 2.

Moreover, the societal concern of tracking the movements of individuals in and out of their homes, as noted in *Knotts* and *Jones* carries little weight in this case. *See Jones*, 565 U.S. at 430; *Knotts*, 460 U.S. at 281. The restrictive time frames outlined in the court order were specifically curtailed to only pinpoint the possible times when the ATMs were accessible, and thus could have been tampered with. *See* Hale Aff. #17. They are also limited to the work hours of average individuals. Although Escaton worked part-time as a bartender, the hours of his employment were unspecified, and thus the government officials could not have known for certain when he would be at home, work, or another given location. Minimizing the time frame of the request from 8:00 AM to 6:00 PM was reasonable given these circumstances.

Therefore, the intent of the government was not to track Escaton into his home or to uncover his "familial, political, professional, religious, [or] sexual associations" as in *Jones*, or to assess the activities taking place within the home, as in *Kyllo*. *See Jones*, 565 U.S. at 412; *Kyllo*, 533 U.S. at 34. The officers were not looking at the substance of the conversations either, but rather merely trying to determine whether Petitioner was in the vicinity of the ATMs when the vandalism took place, which is distinguishable from information-gathering techniques like thermal imaging that enable officers to uncover details about activities occurring within one's home that they otherwise would not have access to. *See Kyllo*, 533 U.S. at 34. The intent of the government here was to uncover whether Escaton was perpetrating a scheme to commit financial crimes and identity theft in the area, with as minimal intrusion as possible.

Similar to the three-day records, even if the weekday records request would ultimately be considered by the Court as an unconstitutional search, we argue that the good faith doctrine applies for the same reasons as listed above.

For the foregoing reasons, the Court should affirm the lower court's decision as to the legality of the weekday records.

VI. ONE HOUR OF CELL TOWER INFORMATION REQUESTED VIA COURT ORDER DOES NOT VIOLATE THE FOURTH AMENDMENT OR THE SCA, AND DOES NOT TRIGGER THE "TRACKING" CONERNS CONTEMPLATED IN *CARPENTER* THAT HISTORICAL CSLI INFORMATION TRIGGERS

The three cell tower dumps orders requested merely one hour of cell tower data – thirty minutes before and after a suspicious man approached the attacked ATMs in Sweetwater. *See* Hale Aff. #19. This request was not only very short in its duration, but also very limited in terms of its geographical reach. *See* R. at 4. This request only yielded a "download of information on all the devices . . . connected to a particular cell site during a particular interval." *See Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021). Therefore, there was no "chronicle of an individual's movements" produced, which is less intrusive than the methods by which CSLI is obtained. *See id.* It also does not "reveal detailed information about a person's life." *See id.*

Moreover, in *Carpenter*, the Court declined to rule on the constitutionality of information obtained via cell tower dumps without a warrant. *See Carpenter*, 138 S. Ct. at 2221. Analogized to static pole cameras as in *Kay*, and distinguished from GPS-like technologies in *Jones*. See *Escaton*, 1001 F.3d (citing *Kay*, No. 17-CR-16, 2018 WL 3995902 at *1); *Jones*, 565 U.S. at 412. Furthermore, the reasonableness of the search, which was not even as intrusive as the data collection within the homes in *Naperville*, is particularly reasonable in this case given the limited scope of the data collection as well as the purpose of catching those engaged in the financial fraud scheme. See *City of Naperville*, 900 F.3d at 528-29.

For the reasons above, the Court should affirm the lower court's decision as to the constitutionality of the three cell tower dumps.

CONCLUSION

Historically, the Court has sought to strike a balance on Fourth Amendment issues between "safeguarding privacy and security of individuals against arbitrary invasions by government official," and prevailing safety concerns. *Camara v. Municipal Court of City and County of San Francisco*, 387 U.S. 523, 528 (1967). Here, officials did not disrupt this balance by conducting a permissible search of Escaton's phone at the border without assistive technology, nor did they do so by obtaining the "Three-Day" and "Weekday" CSLI records and one hour of cell tower dump data in a manner consistent with *Carpenter* and the SCA. For the foregoing reasons, the Court should affirm the Fourteenth Circuit's decision.

Respectfully submitted,

Attorneys for Respondent