No. 10-1011

IN THE

UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT

SPRING TERM 2019

HECTOR ESCATON, *Appellant,*

v.

UNITED STATES OF AMERICA, *Appellee,*

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE FOURTEENTH CIRCUIT

(NO. 1:18-cv-012345)

BRIEF FOR THE RESPONDENT

ON WRIT OF CERTIORI TO THE UNITED STATES SUPREME COURT OF THE UNITED STATES COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT.

TEAM R20

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Constitution, statutes, and rules:

QUESTIONS PRESENTED

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

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

OPINION BELOW

The opinion of the United States District Court for the District of West Texas is reported as *Carpenter v. United States*, 585 U.S. _ (2018).

CONSTITUTIONAL PROVISIONS AND RULES

The Fourth Amendment to 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

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

SUMMARY OF ARGUMENT

The case at bar presents two important issues involving the Fourth Amendment to the United States Constitution. This Court should affirm the circuit court's decision because the Fourteenth Amendment permits forensic searches of the electronic devices at the border without suspicion, as well as the government's acquisition of three days of cell-site information and one-hundred cumulative hours of cell-site location information over two weeks is reasonable pursuant to Carpenter and by Ipso Facto, under the Fourth Amendment.

United States Border Agent Ashley Stubbs conducted the search of Escaton's vehicle when conducting a routine border stop. The Fourth Amendment limits expectation of privacy at border searches simply by virtue of the fact that they occur at the border. In this case, Ashley Stubbs, representing the government, performed the Escaton's vehicle search as a routine procedure. After discovering numerous electronic devices, Agent Stubbs submitted them to a forensic search to search their contents without reasonable suspicion of criminal activity. At that point, Escaton could not claim an expectation of privacy in the electronic devices. Under the search incident to arrest doctrine, Agent Stubbs' submission of electronic devices to forensic search did not violate Escaton's Fourth Amendment right to privacy. Therefore, his actions did not violate the Fourth Amendment.

Furthermore, when Agent Stubbs was performing the search, he found an iPhone, a laptop, three external hard drives, and four USB devices. During that time, he found a paper note that was placed just below the keyboard of the laptop with the message "Call Delores (201)181-0981 $$$".

At this point, despite the fact that an international traveler has limited expectation of privacy, but Escaton's vehicle has showed enough suspicion for the authorities to conduct further advanced searches. It is well established that when an individual crosses an international border, he/she has lesser expectation of privacy because they have been warned in advanced that their belongings, cars and anything that raises the searching officer's suspicion is subject to a thorough search. Here, when Escaton had his electronic devices left visible and/or easily accessible to the searching officer, under the Plain View doctrine, he assumed the risk that an officer would find his electronic devices, and that a suspicion would arise based on the volume of the devices and the notes associated with those devices. Therefore, he did not have an expectation of privacy in his electronic devices. Accordingly, the Circuit Court properly held that Agent Stubbs did not "search" his electronic devices under the Fourth Amendment.

As to the use of cell-site simulators, the tower dumps were instrumental in allowing the FBI to apply for a court order to obtain three-day of Escaton's phone records because his number appeared in the tower dumps records and as stated supra, the number appeared where Mariposa Bank skimming had occurred. The narrow opinion of Carpenter did not address whether the Fourth Amendment is triggered when the government collects cell-site location information from tower dumps.

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

On September 25, 2019, Hector Escaton, a West Texas citizen and resident, returned to the United States from Mexico through a West Texas border checkpoint. Customs and Border Protection (CBP) Officer Ashley Stubbs conducted a routine border search of Escaton's vehicle and found three large suitcases in the back of Escaton's car.

Through his search, Stubbs found an iPhone, a laptop, three external hard drives, and four USB devices. Stubbs placed the iPhone on airplane mode, ensured the laptop was disconnected from wireless service, and manually searched both devices without assistive technology. A paper note was placed just below the keyboard of the laptop with the message "Call Delores (201) 181-0981 $$$." Stubbs recorded the message and the iPhone telephone number and returned the phone to Escaton. However, Stubbs detained the remaining electronic devices, including the laptop, hard drives, and USB devices. No passwords were needed to open the devices. Stubbs discovered that on the laptop, however, certain folders were password protected. Stubbs then inserted the USB devices in the computer and found that he could not access their contents. Stubbs delivered the electronics to Immigration and Customs Enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen who was stationed at the border checkpoint. She used forensic software to copy and scan the devices, which typically takes several hours. Cullen personally examined the results of the forensic program and found that the laptop held documents containing individuals' bank account numbers and pins. The forensic analysis als revealed that the USB devices contained traces of malware. Cullen found no incriminating information on the hard drives and deleted those scans. She reported her findings to Officer Stubbs.

CBP immediately notified the Federal Bureau of Investigation (FBI), which had been investigating "ATM skimming"2 of Mariposa Bank ATMs in Sweetwater during October of 2018.

FBI Special Agent Catherine Hale began examining the connections between the forensic evidence provided by Stubbs and Cullen and that reported by Mariposa Bank. Mariposa Bank operates nationally and owns several branches in Sweetwater. Local branch manager Maeve Millay discovered ATM tampering on October 13, 2018 at the Boswell Street branch after a customer noticed that adjacent ATMs displayed different screens. Millay called the ATM engineer who had examined the Boswell ATMs two days prior. The engineer returned that day and determined that the ATM had been cut open and infected with malware through its USB port. The suspects used the malware to read information from customers who were using the infected ATM terminal. Millay warned the other Sweetwater branches.

A Mariposa Bank internal investigation revealed that skimming occurred at four additional Mariposa ATMs in Sweetwater and three in the neighboring city of Escalante. The Escalante ATMs had been in beta-testing for additional security surveillance, but a malfunction in storage lost all data; Mariposa Bank managers were only able to deduce that skimming occurred in early October 2018. Mariposa Bank determined several methods had been used to steal information and cash from their ATMs. Two of the Sweetwater ATMs had foreign “skimmers” overlaying the ATMs’ debit card readers. Investigators also discovered two additional Sweetwater ATMs with malware installed through a USB port.

Finally, the last ATM had a sophisticated malware that allowed the criminal to empty out the cash at the ATM. ATM maintenance records allowed Mariposa Bank to estimate when the Sweetwater terminals were tampered with. Mariposa Bank estimates $50,000 of losses in October 2018 to the Mariposa Bank and its customers through direct withdrawals and false account creation resulting from ATM skimming. The Bank’s investigation also revealed that hundreds of identities of Mariposa Bank customers were stolen. Mariposa Bank reported its findings to the FBI. Agent Hale received information regarding the malware used and surveillance photographs near the three

ATMs, all of which captured images of a man in a black sweatshirt. Using the forensic search information from CBP and the information provided from the banks, Agent Hale, in coordination with U.S. Attorney Elsie Hughes, requested three tower dumps3 from the cell sites4 near three Sweetwater ATMs pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA)5 for 30 minutes before and 30 minutes after the man in a black sweatshirt approached the ATMs. Stubbs reported Escaton's information, including his telephone number which he found in Escaton's phone, and details to the FBI for potential bank fraud and identity theft claims. The malware found on his USB devices, though not identical, was similar to the malware used at Mariposa ATMs in Sweetwater. Also, his phone number matched one of the numbers generated from the three tower dumps. Based on that information, U.S. Attorney Hughes working with Agent Hale on the investigation applied for court orders under the SCA to obtain Escaton's cell phone records.

A federal magistrate judge issued an order directing Delos Wireless—Escaton's wireless carrier—to disclose "cell site records corresponding to [the] telephone number . . . of Hector Escaton during the period October 11, 2018 through October 13, 2018" (Three-day Records).6 The Three-day Records placed Escaton's cell phone in the area of the Sweetwater Boswell Branch ATM on October 12, 2018. The records, however, did not place Escaton in neighboring Escalante from October 11–13. Suspecting that the "Delores" identified on the paper note in the laptop may have abetted the skimming, the government requested that the magistrate judge issue an additional order to Delos Wireless to disclose "cell/site sector information for Hector Escaton's and 'Delores's' telephone [number] for all weekday records between October 1 and 12 between the hours of 8 AM MDT and 6 PM MDT, as well as all subscriber information for 'Delores's' telephone . . . ."7 (Weekday Records). These records revealed that the phone number belonged to Delores Abernathy during the relevant period and that

she was in the area of the three Escalante ATMs in early October. The CSLI records obtained from Delos also placed Escaton with Abernathy during the same time period. Abernathy had been previously convicted for ATM skimming. After linking Abernathy to the Escalante ATMs, law enforcement indicted her and obtained a search warrant for her house, where they found cash and the same malware that Escaton stored on his USB devices. After Abernathy was arrested, she entered a plea agreement and cooperated with the government in its case against Escaton.

The Government indicted Escaton for 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. Prior to trial in the District of West Texas, Escaton filed a motion to suppress the results of the forensic search and the cell-site data requested from Delos Wireless.9 The district court denied the motion on both issues. Following a jury trial, Escaton was convicted on all charges, and he now appeals.

ARGUMENT

I.

THE FOURTH AMENDMENT PERMITS FORENSIC SEARCHES OF ELECTRONIC DEVICES AT THE BORDER WITHOUT SUSPICION.

We begin with the Fourth Amendment of the United States Constitution principles that govern this case. As a general rule, the Fourth Amendment requires that law enforcement searches be accompanied by a warrant based on probable cause. *Arizona v. Gant*, 556 U.S. 332, 338 (2009). But there are exceptions, and one such exception typically covers our nation's borders. The need for border searches of electronic devices is driven by Custom and Border Protection's (CBP) mission to protect the American people and enforce the nation's laws in this digital age. As the world of information technology evolves, techniques used by CBP and other law enforcement agencies must also evolve to identify, investigate, and prosecute individuals who use new technologies to commit crimes. CBP border searches of electronic devices have resulted in

evidence helpful in combating terrorist activity, child pornography, violations of export controls, intellectual property rights violations, and visa fraud. In furtherance of these critical responsibilities, CBP exercises its border search authority judiciously and in a manner, that preserves the public trust.

At a border – or at a border's "functional equivalent," like the international border at which Escaton was intercepted – government agents may conduct "routine" searches and seizures of persons and property without a warrant or any individualized suspicion. *Almeida-Sanchez v. United States*, 413 U.S. 266, 272–73 (1973); *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). The Supreme Court has described the border exception as "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); see *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004) (border exception rests on government interest in "preventing the entry of unwanted persons and effects"). Routine searches and seizures at the border therefore are exempted from standard Fourth Amendment requirements so that the government can "prevent the introduction of contraband" into the country and bar entry by those who would bring harm across the border, "whether that be communicable diseases, narcotics, or explosives." *Montoya de Hernandez*, 473 U.S. at 537, 544.

Here, the mere reason why Escaton's electronic devices were submitted for forensic search was because of the type of information discovered. As it is known, the level of expectation privacy at international borders are lesser, and one assumes the risk of being searches, because of the warnings before crossing the border. Escaton assumed the risk to cross the U.S. border with incriminating information stored in his electronic devices. It is the duty of the U.S. border patrol officers to protect our nation's interests.

Therefore, despite the fact that the government may conduct a forensic search on the traveler's electronic devices without suspicion, but the traveler himself paved the way to the searching officers to discover the incriminating evidence in his vehicle. Thus, Escaton's Fourth Amendment right not violated, because the amendment permits forensic searches of electronic devices at borders without suspicion.

II.

THE SEARCH OF ESCATON'S ELECTRONIC DEVICES ARE SUPPORTED BY THE TOTALITY OF THE CIRCUMSTANCES DOCTRINE.

The totality of the circumstances test is a standard that considers all of the relevant facts and circumstances, rather than a few specific factors. In this case, the information discovered in the Appellant's electronic devices was the result of a routine border stop. The Unites States Border Agent Stubbs performed the search, and based on what he saw in Escaton's car, he performed a more advanced search of the devices by sending them to Immigration and Customs enforcement (ICE) Senior Special Agent & Computer Forensic Examiner Theresa Cullen. The steps and procedures taken by the government bodies were at no times unreasonable, violation of any individual rights, or out of scope of their duties.

As the court holds in *United States v. Cortez*, 449 U.S. 411 (1981), "When making the determination of whether or not to stop a person, law enforcement must, based on the totality of the circumstances, have a particularized and objective basis for suspecting the particular person of criminal activity." This test manifests itself in two parts. First, this determination must be made based on all available circumstances, specifically objective observations that result in the police officer drawing inferences and making deductions. In the end, this can boil down to common sense conclusions about the potential suspect based on an officer's experience in the field. Second, the officer's objective assessment must raise a suspicion that the person is engaged in criminal activity.

Here, analyzing the first part of the test, taking into account the facts and circumstances presented, Escaton was stopped at a border as part of a routine border check. Second, the searching officer discovered numerous electronic devices, which also contained a paper note reading "Call Delores (201) 181-0981 $$$". Even though the parties agreed that no reasonable suspicion existed at the time of the border search, merely because the border search was a routine search and did not require one, the discovery of the information was the result of that mere responsibility of the border officer to search the traveler's "persons, papers and effect."

As such, because of the totality of the circumstances doctrine, the government had the absolute right to admit into evidence the incriminating evidence obtained as a result of current case's circumstances.

III.

SEARCHES AT THE BORDER ARE REASONABLE WITHOUT SUSPICION "SIMPLY BY VIRTUE OF THE FACT THAT THEY OCCUR AT THE BORDER."

Searches at the border are reasonable without suspicion "simply by virtue of the fact that they occur at the border." *United States v. Alfaro Moncada*, 607 F.3d 720, 728 (11th Cir. 2010) (quoting Denson v. United States, 574 F.3d 1318, 1339 (11th Cir. 2009)). The Supreme Court has held that it is reasonable to conduct without suspicion "[r]outine searches of the persons and effects of entrants" at our borders. U*nited States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985). And we have similarly explained that, at the border, routine "pat-down search[es] or frisk[s]" and searches of "[a] traveler's luggage," "[i]ncoming international mail," and "[v]ehicles" are all reasonable "without any level of suspicion." Alfaro-Moncada, 607 F.3d at 728 (collecting cases). A traveler's "right to be let alone neither prevents the search of his luggage nor the seizure of unprotected, but illegal, materials when his possession of them is discovered during . . . a search." Thirty-Seven Photographs, 402 U.S. at 376 (plurality opinion).

The Supreme Court has never required reasonable suspicion for a search of property at the border, however non-routine and intrusive, and neither have we. Although in one decision the Supreme Court required reasonable suspicion for the prolonged detention of a person until she excreted the contraband that she was suspected of "smuggling . . . in her alimentary canal" or submitted to an x-ray or rectal examination, Montoya de Hernandez, 473 U.S. at 541; see also id. at 534– 35, it has never applied this requirement to property. Nor has it "been willing to distinguish . . . between different types of property." Cotterman, 709 F.3d at 975 (Callahan, J., concurring in part, dissenting in part, and concurring in the judgment). Indeed, it held in *United States v. Flores-Montano* that the government may "remove, disassemble, and reassemble a vehicle's fuel tank" at the border without any suspicion. 541 U.S. 149, 155 (2004). It explained that "the 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—simply do not carry over to vehicles." Id. at 152. And it rejected a judicial attempt to distinguish between "routine" and "non-routine" 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." Id.

We have been similarly unwilling to distinguish between different kinds of property. For example, we have upheld "a search without reasonable suspicion of a crew member's living quarters on a foreign cargo vessel that [wa]s entering this country," Alfaro-Moncada, 607 F.3d at 727, even though "[a] cabin is a crew member's home—and a home 'receives the greatest Fourth Amendment protection,'" id. at 729 (quoting United States v. McGough, 412 F.3d 1232, 1236 (11th Cir. 2005)); accord id. at 732. We see no reason why the Fourth Amendment would require suspicion for a forensic search of an electronic device when it imposes no such requirement for a search of other personal property. Just as the United States is entitled to search a fuel tank for drugs, see Flores-Montano, 541 U.S. at 155, it is likewise entitled to search Escaton's electronic

devices. And it does not make sense to say that electronic devices should receive special treatment because so many people now own them or because they can store vast quantities of records or effects. The same could be said for a recreational vehicle filled with personal effects or a tractor-trailer loaded with boxes of documents. Border agents bear the same responsibility for preventing the importation of contraband in a traveler's possession regardless of advances in technology.

Indeed, inspection of a traveler's property at the border "is an old practice and is intimately associated with excluding illegal articles from the country." Thirty-Seven Photographs, 402 U.S. at 376 (plurality opinion). In contrast with searches of property, we have required reasonable suspicion at the border only "for highly intrusive searches of a person's body." Alfaro Moncada, 607 F.3d at 729. Even though the Supreme Court has declined to decide "what level of suspicion, if any, is required for [such] non-routine border searches [of a person]," Montoya de Hernandez, 473 U.S. at 541 n.4, we have required reasonable suspicion for "a strip search or an x-ray examination," Alfaro-Moncada, 607 F.3d at 729. We have defined the "intrusiveness" of a search of a person's body that requires reasonable suspicion "in terms of the indignity that will be suffered by the person being searched," in contrast with "whether one search will reveal more than another." *United States v. Vega-Barvo*, 729 F.2d 1341, 1345 (11th Cir. 1984); accord id. at 1346. And "we have isolated three factors which contribute to the personal indignity endured by the person searched: (1) physical contact between the searcher and the person searched; (2) exposure of intimate body parts; and (3) use of force." Id. at 1346. These factors are irrelevant to searches of electronic devices.

A forensic search of an electronic device is not like a strip search or an x-ray; it does not require border agents to touch a traveler's body, to expose intimate body parts, or to use any physical force against him. Although it may intrude on the privacy of the owner, a forensic search

of an electronic device is a search of property. And our precedents do not require suspicion for intrusive searches of any property at the border. See Alfaro-Moncada, 607 F.3d at 728–29, 732.

IV.

THE GOVERNMENT'S ACQUISITION OF THREE DAYS OF CELL-SITE INFORMATION AND ONE HUNDRED CUMULATIVE HOURS OF CELL-SITE LOCATION INFORMATION OVER TWO WEEKS IS REAOSNABLE PURSUANT TO CARPENTER AND BY IPSO FACTO, UNDER THE FOURTH AMENDMENT.

The three days of warrantless cell site information and one hundred cumulative hours over two weeks of cell site location information (CSLI)[1] requested of Delos Wireless, a third party, by the FBI pursuant to the Stored Communications Act (SCA) 18 U.S.C. 2703(d), consisted of two individual court orders. The first court order that the FBI requested from Delos Wireless under the SCA was for three days of cell site information corresponding to the telephone number of Hector Escaton (Escaton) during the period October 11, 2018 through October 13, 2018 (Three-day records). The three-day records received from Delos Wireless placed Escaton's cell phone in the area[2] of the Mariposa Bank, Sweetwater Boswell Branch ATM, where the bank skimming had occurred, on October 12, 2018. The second court order for one hundred cumulative hours of cell site location placed Escaton with a cohort but not at another skimmed ATM. *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021.

In *Escaton*, the defendant was searched at a routine border stop in West Texas. The border agent discovered several electronic devices and submitted them to a forensic search which revealed the means and financial information that implicated him in a bank skimming crime of The FBI used the information from the devices and the border patrol agent to request three cell tower

[1] CSLI refers to the information collected as a cell phone identifies its location to nearby cell towers.

[2] CSLI from nearby cell towers can indicate a cell phone's approximate location.

dumps[3], discussed infra at question 2. The tower dumps were instrumental in allowing the FBI to apply for a court order to obtain three-day of Escaton's phone records because his number appeared in the tower dumps records and as stated supra, the number appeared where Mariposa Bank skimming had occurred.

The defendant made a motion for these and the other cell tower records to be deemed inadmissible because they constituted a search in violation of his fourth amendment rights. The Fourteenth Circuit rejected Carpenter's arguments to hold that the records were not protected by the Fourth Amendment.

However, the United States Supreme Court has recently held in *Carpenter v. United States*, 585 U.S. __ (2018), that obtaining seven days' worth of cell tower information requires a warrant, and obtaining this cell tower information through the SCA, was not appropriate.

In *Carpenter v. United States*, 585 U.S. __ (2018), Timothy Carpenter was convicted of robbery after prosecutors presented data from cell-site location information (CSLI) collected from cell phone towers that tracked his movements and put him in the area of several robberies at the time they occurred. The CSLI was obtained by a court order under the Stored Communications Act (SCA). The SCA allows the government to obtain a court order if they "offer specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records, or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d), (herein 2703(d)). Carpenter moved to

[3] A "cell tower dump" provides data about the identity, activity and location of any phone that connects to the targeted cellphone towers over a set span of time, usually an hour or two. A typical dump covers multiple towers, and wireless providers, and can net information from thousands of phones.

suppress the CSLI evidence under the Fourth Amendment, but the district court denied the motion and Carpenter was convicted and he appealed.

The Sixth Circuit rejected Carpenter's argument that the attainment of CSLI through a 2703(d) order was unconstitutional, because it was a search within the meaning of the Fourth Amendment, and a warrant based on probable cause was required. The Supreme Court granted certiorari however their decision produced inherent vagueness, and more questions than answers.

In *Carpenter*, the U.S. Supreme Court answered the question whether the government is required obtain a warrant to access CSLI because it is a search under the fourth amendment. The Supreme Court held "We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment." *Carpenter v. United States*, 585 U.S. __ (2018).

The facts in *Carpenter* are very similar to those in *Escaton* in that they both argued that access to their third party information, because it divulges their whereabouts, required a warrant as delineated in the Fourth amendment. However, it is not certain that the same holding would be reached in *Escaton.*

In *Carpenter,* a narrow decision was made regarding the rules of acquiring CSLI information. More specifically, in a footnote, Roberts stated … "we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."

Carpenter, 585 U.S. at 2217 n 3. At issue in Carpenter was seven days (168 hours) of CSLI which actually only produced two days' worth of information.

Here, Escaton is challenging three days of CSLI. While one-hundred cumulative hours of cell-site location information over two weeks was also requested by the FBI however Escaton did not challenge that court order because they did not place him at the location of the skimmed ATM. Each court order must be viewed separately. The first order is for 72 hours, and the second order, the one hundred hours order was for Court order for Delos Wireless to disclose cell site information for all weekday records between October 1 and 12 between the hours of 8 AM MDT and 6 PM MDT (Weekday Records).

Neither order was for seven days, (168 hours) and only the first order is at issue. The *Carpenter* court made it clear that "It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search", it leaves the question open to speculation whether there is a shorter period of time in which the Government may well obtain CSLI free from Fourth Amendment scrutiny, but the holding makes it appear so.

In his dissent, Justice Gorsuch stated "The Court's application of these principles supplies little more direction. The Court declines to say whether there is any sufficiently limited period of time "for which the Government may obtain an individual's historical location information free from Fourth Amendment scrutiny." *carpenter,* at 2217, n. 3. But then it tells us that access to seven days' worth of information *does* trigger Fourth Amendment scrutiny—even though here the carrier "produced only two days of records." *Carpenter,* at 2217, n. 3. Why is the relevant fact the seven days of information the government *asked for* instead of the two days of information the government *actually saw* ? Why seven days instead of ten or three or one? And in what possible sense did the government "search" five days' worth of location information it was never even sent? We do not know. *Carpenter,* 585 U.S. at 2266-2267. What we do know is that there isn't

justification for advocating that seven days' worth of historical information is a search, while advocating that three days is not a search, because after all, it is the same type of third party information. It has to be noted that seven days of information requested in *Carpenter*, yielded just two days of information. Because of the ambiguity of the Carpenter decision, if may have been more beneficial to create a new classification of handling third party information that contains the privacy information of an individual.

The Supreme Court deviated from its application of the third-party doctrine to CSLI, describing it as "qualitatively different" from the records in *Smith*[4] and *Miller*[5], and "an entirely different species of business record" *Michael Price, Carpenter V. United States and The Future Fourth Amendment* (June 2018). *United States v. Miller* and *Smith v. Maryland* are examples of the application of the third-party doctrine, the legal principle that when an individual voluntarily gives information to a third party, the privacy interest in that information is forfeit. "This is a big doctrinal shift away from how many courts have understood and applied the third-party rule to date. Far from considering the underlying contents or nature of the information at issue, the doctrine has usually worked as a complete bar to Fourth Amendment protection for information shared with third parties…. One notable exception is email. Email "is the technological scion of tangible mail" and it would "defy common sense to afford emails lesser Fourth Amendment protection.". *United States v. Warshak*, 631 F.3d 266, 285-286 (6th Cir. 2010). "The Supreme

[4] In *Smith v. Maryland*, the Court held that police did not require a warrant to use a pen register to monitor a suspect's outgoing call data.

[5] In *United States v. Miller,* the Court held that a defendant had no right to privacy in his banking records, as they were business records belonging to the bank.

Court has never ruled directly on this issue…" *Michael Price, Carpenter V. United States and The Future Fourth Amendment* (June 2018).

In this digital age where third parties collect and sale our individual personal location and identification information, the Supreme Court was silent on the proper application to protect this information and determine who actually owns the information. The Court did not address, the collection information available from surveillance cameras which allow interested parties to track an individual by using a series of cameras along their route, or license plate readers which track an individual by their route on the highways and freeways.

The Carpenter court was silent as to the constitutionality of the Stored Communication Act and accordingly, it is still valid law. The governments acquisition of less than seven days of cell site records is not addressed by the *Carpenter* holding and thereby ipso facto, three-day records must be allowed to be acquired through the Stored Communication Act, 18 U.S.C.2703 (d).

V.

THE NARROW OPINION OF CARPENTER DID NOT ADDRESS WHETHER THE FOURTH AMENDMENT IS TRIGGERED WHEN THE GOVERNMENT COLLECTS CELL-SITE LOCATION INFORMATION FROM TOWER DUMPS.

The FBI, in coordination with the U.S. Attorney, requested three tower dumps from the cell sites near three Sweetwater ATMs pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act (SCA) for 30 minutes before and 30 minutes after a man in a black sweatshirt approached the ATMs. A cell tower dump provides data about the identity, activity and location of any phone that connects to the targeted cellphone towers over a set span of time, usually an hour or two. A typical dump covers multiple towers, and wireless providers, and can net information from thousands of phones.

The Supreme Court did not opine on whether information requested from a cell tower dump violates the Fourth Amendment. "Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.." *Carpenter v. the United States*, 138 S.Ct. 2206 (2018). Accordingly, cell tower dumps or real-time CSLI still fall under the purview of the Stored Communications Act. As such, a court order for disclosure of cell tower dumps under the Act may be obtained if the government offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of the cell tower dump are relevant and material to an ongoing criminal investigation.

CONCLUSION

For each of the foregoing reasons, we respectfully ask this Court to affirm the Fourteenth Circuit's holding in regards to both issues.

Respectfully Submitted,

Attorneys for Respondent