NO. 10-1011

IN THE

SUPREME COURT OF THE

UNITED STATES OF AMERICA

HECTOR ESCATON,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI FROM THE

UNITED STATES COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT

BRIEF FOR THE RESPONDENTS

Team R6
Counsel of Record
Attorneys for Respondent

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court

United States Courts of Appeals

District Court Opinions

Constitutional Provisions

Legislative Materials

QUESTIONS PRESENTED

I. International border searches constitute a long-established exception to the public's Fourth Amendment rights against unreasonable searches and seizures; does this exception extend far enough to allow government officers in their line of duty to conduct forensic searches at an international border without reasonable suspicion?

II. Whether the Government's acquisition 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 during working hours over two weeks, and cell-site location information collected from cell tower dumps violates the Fourth Amendment in light of the narrow holding in *Carpenter v. United States*.

OPINION BELOW

The United States Court of Appeals for the Fourteenth Circuit issued its opinion on November 2, 2021. The opinion appears on pages 1-16 of the record. The opinion is reported in *Escaton v. United States*, 1001 F.3d 1341 (14th Cir. 2021).

CONSTITUTIONAL PROVISIONS AND RULES

This case involves the Fourth Amendment:

> 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, the United States of America, Appellee in *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 ask the Court to affirm the Fourteenth Circuit's decision below.

Summary of the Argument

The case at bar presents two important issues regarding the Fourth Amendment of the Constitution of the United States of America. This court should affirm the Fourteenth Circuit's decision and deny Petitioner Hector Escaton's motion to suppress because Petitioner has failed to show a Fourth Amendment violation. Neither the forensic search of Petitioner's laptop, hard drives, or USB devices nor the requests for cell-site data violated Escaton's rights under the Constitution.

First, there is a well-established exception to the Fourth Amendment for searches of persons and property at an international border. Escaton was stopped for a routine border search when re-entering the state of West Texas in the United States from Mexico. Customs and Border Protection (CBP) Officer Stubbs conducted a routine border search of Escaton's vehicle and electronic devices. He noticed that he could not access much of the contents of USB drives and laptop files, and turned the devices over to another government official located at the same border checkpoint, who conducted a forensic search. This search was conducted on-site and lasted only a few hours, after which potentially incriminating evidence was discovered linking Escaton to an open investigation about ATM skimming in West Texas. Escaton had checked his right to privacy and security at the metaphorical door when he crossed the border, because individuals have a lesser expectation of privacy at the border due to the need for increased

national security. Reasonable suspicion is not required for officers who are doing their job during a routine border search. Escaton was stopped for a standard search of his car and possessions, thereby making this a routine border search. Therefore, Officer Stubbs needed no suspicion to search Escaton's devices and submit them for forensic analysis.

Even if the forensic search were considered non-routine, which would typically require reasonable suspicion, that requirement should be waived in this case and should not be held to be required of all forensic searches. In previous cases, reasonable suspicion was required for forensic searches that lasted significantly longer than the one in our current case, and typically occurred off-site. Under the plain view doctrine, wherein once something even vaguely incriminating comes up during a routine investigation, Stubbs had reasonable suspicion to order the forensic search. After being unable to access the USB devices or files on the computer, it is only natural that an officer trained to find potential threats to the United States would become suspicious. The United States government has made it very clear that courts should allow officials to do their job without being hindered at the international border, and Stubb's actions were in the interest of public safety and were perfectly reasonable in this case.

None of the cell-site location information (CSLI) obtained by the Government violates Petitioner's reasonable expectation of privacy in light of this Court's narrow holding in *Carpenter v. United States. Carpenter* placed limits on law enforcement's ability to request CSLI through the Stored Communications Act (SCA), but did not wholly ban the government from getting CSLI via the SCA. The Court held that obtaining seven-days' worth of CLSI via the SCA violated the Fourth Amendment. The Weekday Request totals 100 hours, and the Three-Day Request totals 72 hours. Accordingly, neither request violates the narrow holding of *Carpenter*.

The privacy concerns implicated by the Weekday Request is more akin to *United States v. Knotts*. The Court held in *Knotts* that an individual traveling on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. As the Weekday Request concerns location information from 8 AM to 6 PM on weekdays, when people are in the public thoroughfare, Escaton's reasonable expectation of privacy has not been violated.

The Three-Day Request similarly does not violate the Fourth Amendment because it does not provide an intimate window into Escaton's life. The 72 cumulative hours of the Three-Day request at best constitute a brief, incomplete snapshot of Escaton's movements. The *Carpenter* court was concerned with near-perfect surveillance, which this does not rise to the level of.

Finally, tower dumps merely reveal a single location and thus there is no need to add an increased level of scrutiny under *Carpenter*. Tower dumps do not provide a chronicle of an individual's past movements, and therefore implicate none of the privacy concerns that the CSLI from *Carpenter* did. Further, tower dumps are crucial during the early stages of investigations when the Government lacks the evidence necessary to obtain a warrant. The *Carpenter* court explicitly did not express a view on tower dumps nor call into question conventional surveillance techniques and tools, which tower dumps are.

Standard of Review

This Court deems questions of law reviewable under a de novo standard. *Pierce v. Underwood*, 487 U.S. 552, 558 (1988). Both issues on review address constitutional questions of law regarding the definition and scope of a search under the Fourth Amendment and therefore, the standard of review is de novo. *See Wright v. West*, 505 U.S. 277, 297-298 (1992) ("[W]e adhered to the general rule of *de novo* review of constitutional claims . . .").

STATEMENT OF THE CASE

Statement of Facts

On September 25, 2019, Hector Escaton ("Escaton") stopped at an international border checkpoint on the border of the state of West Texas, where he is a resident and citizen, and Mexico. (R. at 2). Customs and Border Protection Officer Ashley Stubbs ("Stubbs") conducted a routine border search of Escaton's vehicle. (R. at 2). Among Escaton's belongings Stubbs found an iPhone, a laptop, three external hard drives, and four USB devices. (R. at 2). Stubbs thoroughly searched the many electronic devices, being careful to place the iPhone on airplane mode, and disconnecting the laptop from wireless service. (R. at 2). Stubbs searched all of these devices without assistive technology. (R. at 2).

The first thing Stubbs noted was that there was a note placed below the keyboard of the laptop that had written on it "Call Delores (201) 181-0981 $$$." (R. at 2). Stubbs continued to search and found that certain folders on the laptop were password protected, and that he was completely unable to access any of the contents on all of the USB drives. (R. at 3). Stubbs decided that this required further investigation and brought the electronics (except for the iPhone) to Immigration and Customs Enforcement Senior Special Agent & Computer Forensic Examiner Theresa Cullen ("Cullen"), who was stationed at the same border checkpoint location.

Cullen used forensic software to to scan the devices and found that the password protected files on the laptop contained individuals' bank account numbers and pins. (R. at 3). The software also revealed that the USB devices contained traces of malware, which can be used in the process of "ATM skimming," the process of stealing individuals' bank account information through ATMs. (R. at 3). A forensic software search typically takes several hours.

(R. at 3). Cullen reported her findings to Officer Stubbs, who in turn notified the Federal Bureau of Investigation ("FBI"). (R. at 3).

The FBI had been involved in investigating ATM skimming at Mariposa Bank in Sweetwater since October, 2018. (R. at 3). FBI Special Agent Catherine Hale ("Hale") examined the connection between Escaton and Mariposa. (R. at 3). The investigation began when a local branch manager discovered ATM tampering on October 13, 2018, after a customer reported a discrepancy between several ATMs. (R. at 3). The branch manager called back the engineer who had examined the ATMs two days prior. (R. at 3). The engineer determined that malware had been used to infect the ATM through its USB port to read bank account information from customers who were using the ATM. (R. at 3). Additional investigation showed that several other ATMs in four locations in Mariposa banks in Sweetwater and three locations in the neighboring city of Escalante had also been subject to skimming. (R. at 3). Several more of the locations had received the malware treatment, while a few others had foreign "skimmers" installed over the credit or debit card reading devices. (R. at 4).

Mariposa Bank estimates $50,000 of losses in October 2018 as a result of the ATM skimming. (R. at 4). The investigation also revealed that individuals' identities were stolen during this time as well. (R. at 4). Hale obtained surveillance photos from security cameras near three of the ATMs, all of which showed a man in a black sweatshirt. (R. at 4). After receiving the new information from Officer Stubbs, Hale, in coordination with U.S. Attorney Elsie Hughes ("Hughes") requested three tower dumps from the cell sites near the three Sweetwater ATMs. (R. at 4). They did this pursuant to 18 U.S.C. § 2703(d) of the Stored Communications Act ("SCA"), and requested the 30 minutes prior to and the 30 minutes after the man in the black sweatshirt approached the ATMs. (R. at 4). Hale concluded that the malware that was found in Escaton's

phone was similar to the malware used to infect the ATMs, and Escaton's phone number was revealed as one of the numbers generated from the three tower dumps. (R. at 5).

Hughes and Hale then worked together to get a court order from a federal magistrate judge instructing 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). (R. at 5). These records placed Escaton in the area of one of the ATMs in Sweetwater on October 12, 2018. (R. at 5). Because the records did not place Escaton in neighboring Escalante at this time, Hale and Hughes requested that Delos Wireless 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 (Weekday Records), as well as subscriber information for 'Delores's' telephone…" using the information they had received from Officer Stubbs about Delores' phone number. (R. at 5). The records revealed that the phone number belonged to Delores Abernathy ("Abernathy") and the CSLI data revealed that both Abernathy and Escaton were in the area of the Escalante ATMs during the same time period in early October. (R. at 5). Abernathy has previously been convicted for ATM skimming. (R. at 5).

The government arrested Abernathy and she cooperated with them in the case against Escaton. (R. at 5). 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. (R. at 6). Escaton has filed a motion to suppress the results of the forensic search and the cell-site data. (R. at 6). The district court denied the motion on both issues. (R. at 6). He appealed, and the Court of Appeals for the Fourteenth Circuit affirmed the decision of the district court on both counts. (R. at 14). This appeal followed.

ARGUMENT

I. THIS COURT SHOULD AFFIRM BECAUSE THE FOURTH AMENDMENT BORDER EXCEPTION DOES NOT REQUIRE THAT GOVERNMENT OFFICERS HAVE REASONABLE SUSPICION BEFORE CONDUCTING SEARCHES OF ELECTRONIC DEVICES AT AN INTERNATIONAL BORDER.

A. The search of Petitioner's electronic devices was part of a routine border search and such searches historically do not require reasonable suspicion.

The Supreme Court of the United States has declined to rule in favor of upholding a reasonable suspicion requirement before officers can search personal property at any United States border. *United States v. Cotterman*, 709 F.3d 952, 971 (2013). In fact in all its history of addressing border search cases of personal property only once has the Supreme Court ruled in favor of even a basic requirement of reasonable suspicion. *Id.* This was a very specific case involving drugs carried within a woman's alimentary canal, which involved a long period of detention, hospitalization, and invasive procedures done on the woman's person. *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985). Generally in cases of personal property, the Supreme Court has yet to go so far, and has shown no inclination to do so. If anything, they have indicated the opposite intention.

The Fourth Amendment of the United States Constitution guarantees citizens of the United States "The right…to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" U.S. Const. amend. IV. The key phrase here is "unreasonable," implying that the test when considering cases under the Fourth Amendment is whether or not the search or seizure is reasonable. However, there exists an exception to the Fourth Amendment when it comes to searches at any international border or its functional equivalent. *Cotterman*, 709 F.3d 952 at 960. This exception has existed since before the

inception of the Fourth Amendment, rooted in "the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). Protection and defense are key considerations at any international border, and government officials need to be able to do their jobs and stop illegal contraband from entering the country. Border checkpoints may be the only chance any officer has in finding such contraband.

Because of this heightened interest of the government in protecting and preserving national security at the nation's borders, the Supreme Court has stated that the government interest is "at its zenith at the international border." *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004). They go on to state that stops and searches made at the border "are reasonable simply by virtue of the fact that they occur at the border." *Id.* "The United States, as sovereign, has the inherent authority to protect, and a paramount interest in protecting, its territorial integrity." *Id.* at 153. We want our government to be able to protect its citizens in cases of national emergency or against potential threats, and limiting the government's rights at the border would severely impair their ability to do so.

Courts differentiate between "routine" and "non-routine" customs searches. *Cotterman*, 709 at 961. A routine customs search is "analyzed as a border search" and requires neither probable cause nor reasonable suspicion. *Id.* The facts in this case plainly indicate that Petitioner underwent a routine border search; he was stopped at an international checkpoint when returning to the country, and he had all of his belongings searched at the checkpoint. (R. at 2). Petitioner was not even subjected to a more invasive body search, such as the one that occurred in the first case in which the Supreme Court distinguished between routine and non-routine searches, *United States v. Montoya de Hernandez*. 473 U.S. 531 (1985). They state very plainly that routine

searches are not subject "to any requirement of reasonable suspicion." *Id.* at 538. This is also the first case where the Supreme Court addresses what level of suspicion is required for anything other than a routine border search, so termed non-routine. They hold that such non-routine border searches are justified if customs officials have reasonable suspicion—however they very narrowly hold this in the context of someone smuggling drugs in their alimentary canal. *Id*. at 541. The Supreme Court has never addressed what a non-routine search would be considered in the context of technology.

Though the Supreme Court has never addressed this issue directly, the 4th Circuit has ruled on a very similar issue. In *United States v. Kolsuz*, the 4th Circuit Court of Appeals ruled that a non-routine border search at least requires some level of individualized suspicion. *United States v. Kolsuz*, 890 F.3d 133 (2018). Mr. Kolsuz was detained at an airport after customs officials found firearm parts in his luggage, and he had his luggage as well as his electronics searched at this functional equivalent of a border. *Id*. at 136. The officials then arrested him, and after his arrest they took possession of his phone and subjected it to a month-long forensic search offsite. *Id*. This was considered to be a non-routine border search. *Id.* "Under *Riley*, the forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion." *Id*, at 137, citing *Riley v. California*, 134 S. Ct. 2473 (2014).

Petitioner's case can be differentiated from *Kolsuz* in several ways. Though a forensic search was conducted on Petitioner's laptop, it was done at the same border checkpoint where he was stopped, and took merely a few hours, as opposed to being taken away for a month. (R. at 3). The forensic search was only conducted after Officer Stubbs realized there were password protected files on the computer that he could not access, and he had no access at all to the several

USB devices that Petitioner carried. (R. at 2). He also had observed the note under the laptop's keyboard stating to call Delores for "$$$" and listing a phone number. (R. at 2). His natural instinct was to continue investigating, and the entire process occurred on site at the border during the same day. (R. at 3). It is unlikely the 4th Circuit court would consider Petitioner's border search as anything other than routine, given that it did not involve depriving Petitioner of necessary technology for a significant period of time.

The Fourth Circuit also relied on the Supreme Court logic from *United States v. Flores-Montano* when making their distinction between routine and non-routine. In *Flores-Montano* the court held that there were three major factors that should influence lower courts when making this decision: 1) Whether the search involves a procedure that is a highly intrusive search of a person 2) Whether the search involves a destructive search of property and 3) Searches conducted in a particularly offensive manner. *United States v. Flores-Montano*, 541 U.S. 149 (2004). It is the third factor the *Kolsuz* court relies on when making their judgment of whether or not the border search in that case was routine or not, stating that the extended search of Kolsuz's cell phone which deprived him of his technology for a month was too invasive. *Kolsuz*, 890 F.3d 133 at 140.

Applying the *Flores-Montano* factors, Petitioner's search would be considered routine. This was not a search of Petitioner's person in any way, and therefore factor one is inapplicable. No destruction of property occurred; though they searched Petitioner's laptop and USB devices they did not delete or tamper with any information. (R. at 3). Neither was this a particularly offensive search. Petitioner was stopped during a routine border check. (R. at 2). His devices were searched, and when Officer Stubbs saw that there were a suspicious number of password protected items that he could not access in Petitioner's technology, he submitted the search to a

forensic analyst on site. (R. at 3). Petitioner was only without his devices for a few hours, during which time his phone was returned to him and not subjected to a forensic analysis. (R. at 3). There is no indication in the Record that Petitioner voiced any complaint or objection to his devices being subjected to forensic analysis. Comparing this case directly to *Kolsuz*, Petitioner was deprived of his laptop and USB devices for a significantly shorter period of time for the sole purpose of accessing the protected files, which Officer Stubbs was unable to do with his technological capabilities. (R. at 3). Once the files were accessed, the findings were reported for further investigation "immediately". (R. at 3). Nothing offensive occurred here, and therefore factor three is inapplicable. With all three factors ruled out, according to the Supreme Court, Petitioner's border search would be considered routine.

Though most of the other circuits have not addressed directly the issue of whether a search is routine or non-routine, many have ruled on what kinds of searches they allege to require reasonable suspicion. Currently no reasonable suspicion is required for shipping containers, pat-downs, or even living quarters on ships. *Bradley v. United States*, 299 F.3d 197 (3d Cir. 2002), *United States v. Ajlouny*, 629 F.2d 830 (2d Cir. 1980), *United States v. Alfaro-Moncada*, 607 F.3d 720 (11th Cir. 2010), This last aspect is especially important, because the home is entitled to the most stringent Fourth Amendment protection, and a cabin is a person's equivalent of a home while they are at sea. *Alfaro-Moncada*, 607 F.3d 720 at 729. If the equivalent of a home does not require reasonable suspicion to be searched when entering the United States, a laptop hardly can be accorded a higher standard of suspicion. Searching one's laptop even as thoroughly as possible is not the same as violating Petitioner's right to privacy in his home, or on his person.

Based on all of the case law presented above and the precedents previously held by the Supreme Court, it is highly unlikely that Petitioner's stop would be considered anything other than routine. He was held for a fairly minimal amount of time, and nothing too invasive occurred. (R. at 3). The Supreme Court has never directly ruled on border searches when it comes to technological devices, but has emphasized that at the border the Government has more power. *Montoya de Hernandez*, 473 U.S. 531 at 540. "The Fourth Amendment balance between the interests of the Government and the privacy right of the individual is also struck much more favorably to the Government at the border." *Id*. Because this was nothing more than a routine border search, and Officer Stubbs is charged with protecting our nation at its borders, no level of reasonable suspicion should be required for this case.

B. If the forensic search of Petitioner's electronic devices is to be considered non-routine, no level of reasonable suspicion should be required.

If this court decides to rule that Petitioner's search was non-routine merely on the basis that it was a forensic search at our nation's border, they should still hold that no level of reasonable suspicion was required in this case. The Supreme Court has never ruled directly on this issue, however as stated above, they lean heavily towards allowing the government to do their jobs at the border. The 11th Circuit in the case of *United States v. Touset* ruled on a very similar issue that no level of reasonable suspicion whatsoever is required for forensic searches of an electronic device at the border. *United States v. Touset*, 890 F.3d 1227 (11th Cir. 2018). They clearly state that "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." *Id*. at 1233. The 11th Circuit had previously required reasonable suspicion for a strip search and an x-ray examination, following the factors set forth in *Flores-Montana*. *Id*. at

1234. They also point out that in the past, the Supreme Court has not distinguished between routine and non-routine, and has refused to craft "[c]omplex balancing tests." *Id*. 1233, quoting *Flores-Montana*, 541 U.S. 149. This court should follow the 11th Circuit's logic and refuse to create ever more complex rules and regulations restricting government actions at our border, and thereby potentially infringing upon the government's ability to keep its citizens safe.

The main goal of the government at the border is to promote national safety and security. The Eleventh Circuit points out that if they were to require reasonable suspicion for forensic searches it would create a special protection for the property most used to store illegal information. *Id*. Technology is an ever evolving, ever changing and ever more necessary part of our daily lives, and people store more and more of their information within it. However, again, it is no different from any other form of property. People can choose what to bring across the border with them, also with the full knowledge that they will be subjected to a more intense scrutiny when crossing. Ruling in favor of a no reasonable suspicion standard has no downside; if people aren't carrying anything illegal across the border, the most they have to worry about is spending a little more time there to clarify that they are not bringing anything illegal across. If they are, it is a much better outcome if the government catches them at the border and takes care of it in the easiest manner possible.

The Ninth Circuit has also ruled on this matter; they held that reasonable suspicion is required when the Government conducts a forensic search. However again, the facts of this case can be differentiated from our own. In *United States v. Cotterman* authorities took Cotterman's laptop away from him for days while they conducted a forensic search in an offsite location. *United States v. Cotterman*, 709 F.3d 952 (2013). However the dissent in *Cotterman* makes more persuasive points than the majority. *Id*, at 971. They point out that as the Supreme Court has held

time and time again, searches at the border are per se reasonable, meaning that they do not require reasonable suspicion. *Id*. Though the majority makes the point that people can now carry a wealth of information in their technology, and this of course crosses the border with them if they so choose, the dissent points out that "a port of entry is not a traveler's home" and therefore not subject to as much Fourth Amendment protection, even if the traveler decides to carry a home's worth of information across it. *Id*, at 977. The dissent in *Cotterman* also points out that a bright-line rule is just the sort the Supreme Court has made clear has no place in Fourth Amendment jurisprudence. *Cotterman*, 709 F.3d 952 at 978.

In the case of *United States v. Seljan* the Ninth Circuit held that opening someone's mail requires reasonable suspicion, but they ultimately ruled that reasonable suspicion existed in that case. *United States v. Seljan*, 547 F.3d 993 (9th Cir. 2008). They liken their reasoning to what they call the plain view doctrine; after obtaining a warrant to search an area if police discover evidence of a different crime they are allowed to search for evidence of this other crime as well. *Id*. Once the officer had observed something suspicious about the mail, which is within his jurisdiction as the postal inspector, he was within his rights to open it and search for further incriminating evidence. *Id*. This principle applies to our current case as well. Once Officer Stubbs had accessed Petitioner's phone and laptop after disconnecting them from Wifi, he saw password protected files and USB drives that he was unable to access, as well as the note about calling Delores for money. (R. at 3). Naturally, this would arouse anyone's suspicion. Doing his job, he submitted the laptop and USB drives to a forensic search, where illegal material was discovered on them. (R. at 3). Officer Stubbs was well within his rights to look through Petitioner's laptop and USB drives with the Wifi disconnected, that is not disputed based on the border search exception from the Fourth Amendment as discussed above. Once he has that right,

the plain view doctrine would allow him to continue searching if he found anything suspicious, just what happened here. The *Seljan* court held this to be their reasoning, and though they did ultimately require reasonable suspicion to be necessary, here after Officer Stubbs had initially looked through the files and found something suspicious he had enough reasonable suspicion to continue his search.

If this court decides to hold that this was a non-routine border search, based on the reasoning of the Supreme Court and the cases listed above, this court should still not find that reasonable suspicion is required, or if they do, they should follow the reasoning of *Seljan* and find that there was sufficient reasonable suspicion here.

II. THIS COURT SHOULD AFFIRM BECAUSE THE GOVERNMENT'S ACQUISITION OF THE CELL-SITE LOCATION INFORMATION OF PETITIONER COMPLIES WITH *CARPENTER* AND DOES NOT VIOLATE THE FOURTH AMENDMENT

A. *Carpenter* affirmed law enforcement's ability to request cell-site location information (CSLI) under the Stored Communications Act (SCA)

The Stored Communications Act (SCA) authorizes a Magistrate Judge to issue an order requiring disclosure of cell-site records if the Government demonstrates "specific and articulable facts showing that there are reasonable grounds to believe" the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). The holding in *Carpenter v. United States* merely placed limits on law enforcement's ability to request cell-site location information (CSLI) via the SCA; namely that an SCA request for seven days' worth of CSLI violates an individual's reasonable expectation of privacy. *Carpenter v. United States*, 138 S. Ct. 2206, 2217 n.3 (2018). Modern devices such as smartphones, tap into wireless cell site towers to generate a signal. *Id.* at 2211. Each time the phone connects to a cell site, it generates a time-stamped record known as CSLI, reflecting the location of the tower it connected to. Imposing

additional restrictions would serve an adverse purpose and nullify Congress' reasonable framework for obtaining cell-site records in some of the most serious criminal investigations. *Id*. at 2233 (Kennedy, J. dissenting).

In the present case, the government followed all procedures under the SCA and met the standard articulated within the statute. *see* Hale Affidavit. Agent Hale's Affidavit in Support of the § 2703(d) order offers specific and articulable facts showing that there are reasonable grounds to believe that the CSLI records for Petitioner are relevant and material to an ongoing criminal investigation. *Id*. The affidavit explains that five ATMs were tampered with in Sweetwater, and three ATMs were tampered with in Escalante. (R. at 3). The ATMs in question had either malware installed or contained foreign skimmers. (R. at 4). The search of Petitioner's electronics revealed malware similar to those used at the ATMs, and personal banking information of many individuals. Foreign skimmers operate by pulling the personal banking information from individuals who use that ATM. (R. at 3 n.2). Further, through the tower dumps, Agent Hale knew that Petitioner's phone was located near one of the infected ATMs within thirty minutes of a man in a black sweatshirt approaching the ATM. (R. at 4-5). Thus, the Government has demonstrated specific and articulable facts showing that there are reasonable grounds to believe the CSLI records for Petitioner are relevant and material to an ongoing material investigation, and the standard Congress articulated under 18 U.S.C. § 2703(d) is met.

Indeed, central to the holding in *Carpenter* was the reasoning that the Court should reject a mechanical interpretation of the Fourth Amendment. *Carpenter* 138 S. Ct. at 2214; *see also Kyllo v. United States*, 533 U.S. 27, 35 (2001). To reason that since *Carpenter* held that seven-days' worth of CSLI constituted a search under the SCA, that it deemed any CSLI request via the SCA a search would be a mechanical interpretation in the truest sense of the word. The Court

was explicit in their narrow holding that they were merely deciding that a week's worth of CSLI was a search. *Carpenter*, 138 S. Ct. at 2217 n.3. To invalidate subsequent valid CSLI orders via the SCA because of *Carpenter's* narrow holding would offend the very notion of avoiding a mechanical interpretation of the Fourth Amendment that the *Carpenter* Court was so concerned with.

During periods of rapid technological advancement, particularly where the governing legal standard is one of reasonableness, it is wise to defer to legislative judgements. *See United States v. Jones*, 565 U.S. 400, 430 (Alito, J., concurring) (2012). A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way. *Id.* It is therefore proper to defer to Congress to determine the appropriate standard, which is currently embodied in § 2703(d) of the SCA. Alternatively, the Senate currently has a bill to amend the SCA to require a search warrant for geolocation data. (R. at 12). In fact, Congress has amended the SCA in the past when it deemed changes necessary. In 1994, Congress amended the SCA to impose the new "specific and articulable facts" standard regarding cell-site records. *See* Pub. L. No. 103-414, Title II, § 207(a) (1994). If changes are to occur to a CSLI request under the SCA, that determination is best left to the Legislature, and not judges engaging in judicial activism.

Further, the *Carpenter* held that there aren't limitations on obtaining CSLI through the SCA during when "the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable." *Carpenter* at 2222. The case at bar presents such a situation. This case involves the criminal practice of ATM skimming, which costs U.S. banks hundreds of millions of dollars annually and affects thousands of bank

customers. (R. at 3 n.2). The crime in question is not a run-of-the-mill scam, but an organized criminal operation which plagues our society if left unimpeded.

B. The Weekday and Three-Day CSLI requests do not violate the Fourth Amendment in light of *Carpenter's* narrow holding

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable search and seizures, shall not be violated." U.S. Const. amend. IV. Fourth Amendment jurisprudence was originally tied to common law trespass, until the latter half of the 20th century. *Kyllo*, 533 U.S. at 31. However, in *Katz v. United States*, the court recognized that the Fourth Amendment protects people, not places. *Katz v. United States*, 389 U.S. 347, 351 (1967). The prevailing standard, from Justice Harlan's concurrence in *Katz*, states that a Fourth Amendment violation occurs when the government violates a person's reasonable expectation of privacy. *Id*. at 360 (Harlan, J., concurring).

In *Carpenter v. United States*, the Court held that law enforcement conducts a search under the Fourth Amendment when the government obtains seven days of historical cell-site records to create a detailed account of the user's past movements. *Carpenter*, 138 S. Ct. at 2217 n.3. The majority in *Carpenter* were careful to craft an explicitly narrow holding, stating that "…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." *Id*. The Court reasoned that when the Government requests seven days' worth of cell-site location information, an individual's reasonable expectation of privacy is violated. *Id*. The Weekday request is for a mere 100 cumulative hours and the Three-Day request totals 72

hours, while the *Carpenter* request totaled 168 hours. (R. at 5 n.7). Thus, the Weekday and Three-Day requests do not violate *Carpenter's* narrow holding.

i. The Weekday request does not implicate the same privacy concerns that the seven-day request from *Carpenter* does

The Court in *Carpenter* outlined two guideposts to determine unreasonable searches and seizures: "to secure the privacies of life against arbitrary power" and "to place obstacles in the way of a too permeating police surveillance." *Carpenter*, 138 S. Ct. at 2214. The Court was concerned that the seven-day CSLI records violated the basic goalposts to determine Fourth Amendment violations by creating a detailed account of an individual's past movements, especially by revealing the individual's familial, political, religious, and sexual associations. *Id*. at 2217. The Weekday records, by their very nature, reveal no such information. The Weekday records requested from Delos Wireless only contain cell-site location information from 8 AM MDT to 6 PM MDT. (R. at 5). Not only are the 100 total hours requested from the Weekday less than the 168 hours requested from *Carpenter*, the records are also much less invasive. The Weekday records occur during business hours when people are typically in the public domain. This amounts to less than five days' worth of hours during the relevant time frame. (R. at 13). Thus, the carefully narrow holding of *Carpenter* is not violated, as the Weekday records are not only less than seven days' worth of CSLI, they are also much less invasive.

Limiting the request to working hours greatly diminishes the privacy concerns implicated in *Carpenter*. The majority was gravely concerned that a cell phone follows its owner beyond public thoroughfares and into private residences and other sensitive environments. *Carpenter*, 138 S. Ct. at 2218. The Weekday records certainly does not achieve near perfect surveillance "as

if it had attached an ankle monitor to the phone's user." *Id*. Accordingly, the Weekday records do not violate Petitioner's reasonable expectation of privacy.

The privacy interest at bar is much more akin to *United States v. Knotts*. In *Knotts*, the Court held that the government's warrantless use of a beeper to track a vehicle through traffic did not violate that individual's reasonable expectation of privacy. *United States v. Knotts*, 460 U.S. 276, 285 (1983). The Court reasoned that an individual traveling on public thoroughfares has no reasonable expectation of privacy in his movements. *Id*. at 281. The electronic surveillance in *Knotts* did not amount to a search because it merely revealed information that could be discovered from a public thoroughfare. *Id.* at 284.

All CSLI information regarding Petitioner's whereabouts revealed via the Weekday Request ostensibly occurred in the public thoroughfare. As the Weekday records were from 8 AM to 6 PM on weekdays, when people are generally working, all the information revealed during the short time period requested would have been available to law enforcement absent surveillance. Unlike in *United States v. Karo*, another beeper tracking case where the government tracked inside numerous private residences and storage facilities, the cell-site information from the Weekday records will only reveal information during working hours, where people are in the public thoroughfare. *See United States v. Karo*, 468 U.S. 705 (1984) (holding that warrantless monitoring of a beeper in a private residence, a location not open to visual surveillance, was a search). A person has no reasonable expectation of privacy in their location in the public, and therefore the Weekday Records, like the location tracking in *Knotts*, are not a search under the Fourth Amendment.

However, the Court in *Knotts* did recognize that different constitutional principles may be applicable to certain "dragnet-type" law enforcement practices. *Knotts*, 460 U.S. at 284. But, the

Court was making reference to twenty-four-hour surveillance of an individual without judicial knowledge or supervision. *Id.* at 283. These different constitutional principles do not apply to the present case. First, the Court was concerned about twenty-four hour surveillance. *Id*. at 283-285. The Weekday records do not constitute twenty-four hour surveillance as they are confined to working hours. (R. at 5). Second, The SCA requires that a neutral Magistrate Judge find that the Government has reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation. 18 U.S.C. 2703(d). Accordingly, this judicial oversight distinguishes the present case from the "dragnet type" law enforcement practices without judicial knowledge or supervision that concerned the court in *Knotts*. This judicial check mitigates the Court's concerns about a too permeating police surveillance.

This Court's Fourth Amendment jurisprudence also makes clear that "we must assure preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, 533 U.S. at 34. The Weekday records, analogous to viewing an individual while they are in the public thoroughfare during working hours, does not offend the degree of privacy that existed in the early history of this country. The Weekday records reveal information between the hours of 8 AM and 6 PM. (R. at 5). This information shows Petitioner's movements in the public thoroughfare, where individuals have no expectation of privacy in their movements. *Knotts,* 460 U.S. at 281. This is true now, and it was true when the Fourth Amendment was adopted. Accordingly, the weekday records assure preservation of the degree of privacy against government that existed when the Fourth Amendment was adopted.

Further, the cell-site tower location information is imprecise, and does not "achieve near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Carpenter*, 138 S. Ct. at 2218. While the cell-site location information can be accurate within 50 feet of the

location of the phone in Sweetwater, it is often captured in five to ten-minute increments, which is hardly "perfect surveillance." *See* Hale Affidavit. In Escalante, the location information is even less accurate due to the sparseness of cell towers. *Id*. While it still collects the location information in five to ten-minute increments, the information is often only accurate within 1000 feet of the individual. *Id*. This is a far cry from the accuracy of GPS tracking which the *Carpenter* Court was concerned with.

ii. The Three-Day Records provide a brief, incomplete view of Petitioner's movements, and thus do not provide the intimate window of his life that violates the Fourth Amendment

The Court in *Carpenter* was concerned with longer term monitoring and investigations, regardless of whether the movements were disclosed to the public at large. *Carpenter*, 138 S. Ct. at 2216. While this is a valid concern, the Three-Day records do not constitute long term monitoring, and thus do not rise to the level of impinging on Escalante's reasonable expectation of privacy. The *Carpenter* Court was concerned that the seven-day cell-site information, like the 28 day GPS tracking in *Jones*, provided an intimate window into the defendant's life. *Id*. at 2217. The Court reasoned that these records hold for many Americans the privacies of life and thus should be protected by the Fourth Amendment. *Id*.

The distinction between the present case with *Carpenter* and *Jones* is that the Three-Day records are simply not long term. It is important to note that the Court in *Jones* decided the case on the grounds of the Government's physical trespass of the defendant's SUV in deciding that a Fourth Amendment search had occurred. *Jones* 565 U.S. at 404. In the present case, no such physical trespass has occurred. Nonetheless, the *Jones* Court's concerns on long-term GPS surveillance are important. The *Carpenter* Court determined that it was the accumulation of seven days of records that violated a person's expectation of privacy. *Carpenter*, 138 S. Ct. at

2217 n.3. In fact, the Court reasoned that "mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts." *Carpenter*, 138 S. Ct. at 2217. In *Carpenter*, not only did the Government obtain seven-days' worth of CSLI from Sprint, they also obtained 127 days' worth of records from MetroPCS of Petitioner's location. *Id.* at 2212. Altogether, the Government in *Carpenter* obtained 12,898 location points cataloging Carpenter's movements. *Id.* This is wholly different from the amount of information the Government has obtained on Petitioner. The Government has obtained a mere 72 hours of CSLI on Petitioner via the Three-Day Records. (R. at 2). In the present case, the Three-Day records do not provide an intimate view into Petitioner's life which would violate an individual's privacy. At best, the Three-Day records create a brief, incomplete snapshot of the individual's life.

Additionally, *Jones* was decided by the Government's physical occupation of the individual's private property in order to obtain information. *Jones* 565 U.S. at 404-405. The majority stated that, "it is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information." *Id.* at 404. In the present case, there has been no physical intrusion on Petitioner's property via the cell-site location information requests. In fact, the majority in *Jones* cedes that "visual observation is constitutionally permissible." *Id.* at 412. The CSLI information at issue is analogous to visual observation. Albeit done in a more efficient, electronic manner. But, the Court has "never equated police efficiency with unconstitutionality." *Knotts*, 460 U.S. at 284. The majority opinion in *Jones*, grappling with Justice Alito's concurrence basing the ruling on a violation of reasonable expectation of privacy instead of the Government's physical occupation, observes that it remains unexplained why a 4-week investigation is surely too long. *Jones* 565 U.S. at 412. Similarly, there is no reason to hold that a Three-Day investigation is too long.

Indeed, the Three-Day records are only useful when an officer can specifically link a suspect to the relevant three-day time frame. The records in question would be entirely useless without the maintenance records of Mariposa Bank's Boswell branch and the customer complaint for the ATM which created a three-day window where the ATM tampering occurred. (R. at 3). 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. *Id*. Millay then called the ATM engineer who had examined the Boswell ATMs two days prior. *Id*. Thus, there was a three-day window where the tampering occurred. The malware which infected Mariposa ATMs was similar to the malware found on Petitioner's electronic devices. (R. at 5). The Three-Day request was far from a fishing expedition which provided intimate details into Petitioner's life. The request was narrowly tailored and supported by ample evidence to meet the requirements of the SCA, and the time frame doesn't come anywhere close to offending the narrow holding of *Carpenter*.

While it may be true that through this brief, incomplete snapshot of Petitioner's whereabouts for a mere 72 hours could provide some potential abuse into viewing the intimacies of Petitioner's life the *Carpenter* court was concerned with, the Supreme Court has never held that a potential invasion of privacy constitutes an actual search. *Karo*, 468 U.S. at 712. As the Court in *Karo* recognized, "a holding to that effect would mean that a policeman walking down the street carrying a parabolic microphone capable of picking up conversations in nearby homes would be engaging in a search even if the microphone were not turned on." *Id*. In the present case, there is nothing in the record to suggest that the Government impermissibly violated Petitioner's reasonable expectation of privacy via the Three-Day records. The fact of the matter is that the Government was concerned with placing his location near the ATMs which had been

tampered with. (R. at 5). All of the ATMs are in plain sight, viewable by the public, which doesn't constitute a Fourth Amendment violation. *See Knotts*, 460 U.S. 276. As the *Karo* court articulated, it is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence. *Karo*, 468 U.S. at 712.

C. *Carpenter* should not be applied to tower dumps as they do not provide a chronicle of an individual's past movements and do not violate Petitioner's reasonable expectation of privacy

The Court in *Carpenter* explicitly did not express a view on tower dumps. *Carpenter*, 138 S. Ct. at 2220. A tower dump is a list of every phone number that used a tower for a short period of time. (R. at 4). The tower dump in question included only one hour of cell-tower data for each tower. *Id*. Accordingly, tower dumps implicate none of the privacy corners that cell-site location information does, and *Carpenter*'s holding should not be extended to tower dumps. The record even states that law enforcement only made two warrantless requests: The Weekday request and Three-Day request; leaving out the tower dump request entirely. (R. at 2).

Carpenter should not be applied to CSLI from tower dumps because they do not provide a chronicle of an individual's movements. A tower dump reveals a single location. None of the privacy concerns articulated in the seven day CSLI request in *Carpenter* apply to the tower dump in question. Tower dumps merely provide a download of information on devices that connected to a particular cell site during a particular interval. (R. at 13). This information does not reveal detailed information about a person's life. (R. at 14). The *Carpenter* holding explicitly did not "call into question conventional surveillance techniques and tools," which is exactly what tower dumps are. *Carpenter*, 138 S. Ct. at 2221. It reveals no more than a single location and a cell number, and there is no need to add an increased level of scrutiny under *Carpenter*. *See United States v. Kay*, No. 17-CR-16, 2018 WL 3995902 (E.D. Wisc. Aug. 21, 2018) (finding that 87

days of pole camera footage showing defendant's yard is not a search under *Carpenter* because, unlike a GPS, a pole camera is fixed and doesn't provide an "intimate window" into defendant's life); *see also United States v. Monroe*, 2018 U.S. Dist. LEXIS 186998 (finding that *Carpenter* doesn't apply to IP addresses because it doesn't provide the minutely detailed, historical portrait of the whole of a person's physical movements).

Further, tower dump records are crucial during the early stages of investigations, when the Government lacks the evidence necessary to obtain a warrant. For example, where a murder investigation in its infancy presents multiple suspects with strong motives to commit the crime, a tower dump can eliminate suspects who could not have been in the area. So long as the Government meets the standard under the SCA, which was met here, the requests don't violate the Fourth Amendment. The Supreme Court has not "equated police efficiency with unconstitutionality." *Knotts*, 460 U.S. at 284. Indeed, the Court has recognized the argument that technological devices enabling police to be more effective in detecting crime violates an individual's Fourth Amendment rights has no constitutional foundation. *Id.* Accordingly, the tower dumps shouldn't be analyzed under *Carpenter*, and the tower dumps in question met the SCA standard articulated by Congress, and are thus constitutional.

Moreover, courts have held that tower dumps are ordinary business records of the provider in which the customer has no reasonable expectation of privacy. *See In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *see also In re Cell Tower Records Under 18 U.S.C. 2703(d)*, 90 F. Supp. 3d 67 (S.D. Tex. 2015). Thus, no Fourth Amendment concerns are implicated by the tower dump in question.

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